Федеральное государственное казенное образовательное учреждение высшего образования «Уральский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра криминологии и уголовно-исполнительного права

Организация профилактической работы в сфере противодействия вовлечению детей и подростков в деструктивные интернет-сообщества

Учебно-практическое пособие

Екатеринбург
2021

ББК 67.515
О641

О641 **Организация профилактической работы в сфере противодействия вовлечению детей и подростков в деструктивные интернет-сообщества:** *учебно-практическое пособие*. – Екатеринбург: Уральский юридический институт МВД России, 2021. – 40 с.

ISBN 978-5-88437-825-4

Коллектив авторов: ***Н. В. Голубых***, кандидат юридических наук, доцент;
Ю. А. Западнова, кандидат юридических наук;
Е. В. Щетинина, кандидат философских наук;
А. Л. Пушкарев;
К. А. Акаева;
Н. Л. Кахикало

Рецензенты: **О. В. Ермакова**, доцент кафедры уголовного права и криминологии Барнаульского юридического института МВД России, кандидат юридических наук, доцент;
В. В. Коваленко, начальник организационно-методического отдела управления по вопросам миграции Главного управления МВД России по Свердловской области

Учебно-практическое пособие посвящено особенностям применения форм и методов предупреждения государственными субъектами профилактики вовлечения детей и подростков в деструктивные интернет-сообщества в целях минимизации негативных последствий. Использование учебно-практического пособия позволит повысить уровень знаний и практических навыков, а также достичь эффективных результатов в формировании профессиональных компетенций у обучающихся образовательных организаций системы МВД России.

Издание предназначено для курсантов, слушателей образовательных организаций системы МВД России.

Обсуждено на заседании кафедры криминологии и уголовно-исполнительного права УрЮИ МВД России (протокол № 13 от 1 сентября 2021 г.).

Рекомендовано к использованию в образовательном процессе методическим советом УрЮИ МВД России (протокол № 2 от 18 октября 2021 г.).

ISBN 978-5-88437-825-4 ББК 67.515

Введение

С развитием информационных технологий нарастают угрозы распространения информации, представляющей опасность для детей, обостряются проблемы распространения деструктивных течений. Наиболее актуальной становится тема вовлечения несовершеннолетних в группы экстремистских, националистских и других направлений посредством сети «Интернет».

Для решения данной проблемы на сегодняшний день приняты Концепция развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2025 года [8] и Концепция информационной безопасности детей [7]. Стремительные изменения информационных технологий приводят детей и подростков к принципиально новыми вызовам, ранее не известным ни им самим, ни их родителям. А значит, современное общество не располагает проверенными временем способами правильного и безопасного поведения в новой социальной реальности. Взросление, обучение и социализация детей проходят в условиях «гиперинформационного общества» [7].

Актуальность обеспечения нормального развития детей и защиты их прав также обозначена в последних изменениях Конституции Российской Федерации.

В соответствии с изменениями в Конституцию Российской Федерации от 12 декабря 1993 г., одобренными в ходе общероссийского голосования 1 июля 2020 г., важнейшим приоритетом государственной политики России являются дети (статья 67.1) [1]. Российская Федерация, в соответствии с указанными поправками, берет на себя обязательства по созданию условий для всестороннего духовного, нравственного, интеллектуального и физического развития детей, воспитывая в них чувства патриотизма, гражданственности и уважения к старшим.

Изменения текста действующей Конституции Российской Федерации от 12 декабря 1993 г. оправданы показателями статистических данных в сфере защиты прав несовершеннолетних, регистрируемых Генеральной прокуратурой Российской Федерации. Факты нарушения законов в сфере соблюдения прав и интересов несовершеннолетних за последние 10 лет вызывают обеспокоенность.

Число нарушений законов с 588 тыс. 822 случаев в 2010 г. возросло до 688 тыс. 49 в 2020 г. (рост 16,8 %); в том числе в сфере охраны жизни, здоровья, защиты семьи, материнства, отцовства и детства – с 283 тыс. 952 в 2010 г. до 335 тыс. 102 в 2020 г. (рост 18 %); в сфере профилактики безнадзорности и правонарушений несовершеннолетних – с 90 тыс. 572 в 2010 г. до 116 тыс. 47 в 2020 г. (рост 28,1 %).

Глава 1. Правовая основа противодействия вовлечению детей и подростков в деятельность деструктивных интернет-сообществ

В Российской Федерации принята следующая правовая база в области противодействия вовлечению несовершеннолетних в противоправную деятельность деструктивных интренет-сообществ:

1. Федеральный закон от 24 июня 1999 г. № 120 «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних». Закон устанавливает систему субъектов профилактики безнадзорности и правонарушений несовершеннолетних, определяет их функции, задачи, права и обязанности, формы работы.

В соответствии со ст. 2 данного закона основными задачами субъектов профилактики безнадзорности и правонарушений несовершеннолетних являются:

- предупреждение безнадзорности, беспризорности, правонарушений и антиобщественных действий несовершеннолетних, выявление и устранение причин и условий, способствующих этому;
- обеспечение защиты прав и законных интересов несовершеннолетних;
- социально-педагогическая реабилитация несовершеннолетних, находящихся в социально опасном положении;
- выявление и пресечение случаев вовлечения несовершеннолетних в совершение преступлений, других противоправных и (или) антиобщественных действий, а также случаев склонения их к суицидальным действиям [2].

2. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» устанавливает правила медиабезопасности детей при обороте на территории России продукции СМИ, печатной, аудиовизуальной продукции на любых видах носителей, программ для компьютеров и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях подвижной радиотелефонной связи. Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети «Интернет») вреда их здоровью, физическому, психическому, духовному и нравственному развитию. Также закон устанавливает порядок прекращения распространения продукции средства массовой информации, осуществляемого с нарушением законодательно установленных требований. Каждый выпуск периодического печатного издания, каждая копия аудио-, видеоили кинохроникальной программы должны содержать знак информационной продукции, а при демонстрации кинохроникальных программ и при каждом выходе в эфир радиопрограмм, телепрограмм они должны сопровождаться сообщением об ограничении их распространения [3].

3. Распоряжение Правительства Российской Федерации от 22 марта 2017 г. «Об утверждении Концепции развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2025 года». Данная Концепция отмечает, что особого внимания требуют такие антиобщественные действия, как запугивание, травля ребенка со стороны одноклассников, распространение лживой, порочащей ребенка информации в социальных сетях, которые нередко воспринимаются как норма не только детьми, совершающими противоправные поступки, но и жертвами такого поведения. А также распространение в социальных сетях деструктивной информации [8].

4. Распоряжение Правительства Российской Федерации от 29 мая 2015 г. № 996-р «Об утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года». Данный нормативный правовой акт определяет воспитание детей как стратегический общенациональный приоритет, требующий консолидации усилий различных институтов гражданского общества и ведомств на федеральном, региональном и муниципальном уровнях [9].

5. Постановление Правительства РФ от 26 октября 2012 г. № 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». В данном постановлении закреплен алгоритм принятия уполномоченными органами решений в отношении отдельных видов информации и материалов, распространяемых посредством сети «Интернет», распространение которых в Российской Федерации запрещено [10].

6. Приказ Роскомнадзора № 84, МВД России № 292, Роспотребнадзора № 351, ФНС России ММВ-7-2/461@ от 18 мая 2017 г. «Об утверждении Критериев оценки материалов и (или) информации, необходимых для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерством внутренних дел Российской Федерации, Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека, федеральной налоговой службой о включении доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие запрещенную информацию, в единую автоматизированную информационную систему Единый реестр доменных имен, указателей страниц» [12]. Данный приказ определяет пять критериев оценки запрещенной информации:

– критерии оценки материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера, распространяемых посредством сети «Интернет»;

– критерии оценки информации, о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, аналогов наркотических средств и психотропных веществ, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений, распространяемых посредством сети «Интернет»;

– критерии оценки информации о способах совершения самоубийства, а также призывов к совершению, самоубийства, необходимые для принятия решений, являющихся основаниями для включения доменных имен и (или) указателей страниц сайтов в сети «Интернет»;

– критерии оценки информации об организации и проведении азартных игр и лотерей с использованием сети «Интернет»;

– критерии оценки информации Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций информации, распространяемой посредством сети «Интернет», решение о запрете к распространению которой на территории Российской Федерации принято уполномоченными органами или судом, необходимые для принятия решений, являющихся основаниями для включения доменных имен и (или) указателей страниц сайтов в сети «Интернет», а также сетевых адресов в Единый реестр.

7. Приказ МВД России от 15 октября 2013 г. № 845 «Об утверждении Инструкции по организации деятельности подразделений по делам несовершеннолетних органов внутренних дел Российской Федерации». Отдельную роль в рамках предупреждения вовлечения несовершеннолетних в деструктивные интернет-сообщества отводится подразделениям по делам несовершеннолетних (далее – ПДН), которые проводят с несовершеннолетними правонарушителями индивидуальную профилактическую работу [11].

Сотрудники ПДН в рамках профилактики вовлечения несовершеннолетних в деструктивные интернет-сообщества осуществляют исключительные функции. Так, основной функцией деятельности ПДН, помимо прочих, является выявление лиц, вовлекающих несовершеннолетних в совершение преступления, других противоправных и (или) антиобщественных действий либо склоняющих их к суицидальным действиям, либо к потреблению наркотических средств или психотропных веществ без назначения врача, новых потенциально опасных психоактивных веществ или употреблению одурманивающих веществ, или совершающих в отношении несовершеннолетних другие противоправные деяния.

Стоит отметить, что если деятельность официальных медиа, регламентируется и контролируется на законодательном уровне, то неофициальные информационные источники, распространяющиеся в сети Интернет посредством социальных сетей (аккаунтов, сообществ), не поддаются контролю за счет своей стихийности и массовости, тем самым имея возможность активно распространять и пропагандировать деструктивный контент среди пользователей Интернета.

Вопросы для самоконтроля

1. Охарактеризуйте отечественное нормативно-правовое регулирование деятельности, направленной на противодействие вовлечению несовершеннолетних в деятельность деструктивных интренет-сообществ.

2. Определите, какой нормативно-правовой акт регулирует общественные отношения в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

3. Раскройте критерии оценки запрещенной информации, существующие в Российской Федерации.

Глава 2. Деструктивные интернет-сообщества: понятие, цели, виды, каналы распространения запрещенной информации

Вопросу противодействия деятельности деструктивных интернет-сообществ уделяется внимание даже на уровне первых лиц государства.

Так, 26 февраля 2020 г. Президент Российской Федерации принял участие в ежегодном расширенном заседании коллегии МВД России, где акцентировал внимание на следующем: «в поле вашего постоянного внимания должно находиться и интернет-пространство, в котором продолжают действовать разного рода радикальные группы, пропагандирующие уголовную субкультуру, склоняющие подростков к самоубийствам, совершению правонарушений. Работа по их выявлению должна вестись постоянно, а организаторы и подстрекатели – нести залуженное наказание» [15].

В настоящее время российское общество столкнулось с новыми, тревожными вызовами современности, связанными с деятельностью деструктивных интернет-сообществ, которые влияют на нормальное развитие несовершеннолетних.

Анализ правоприменительной практики, научных взглядов позволяет сформулировать, что под деструктивными интернет-сообществами, как правило, подразумевается неформальная группа или движение, объединенные общими идеалами и интересами, демонстрирующие и романтизирующие опасные формы поведения (суицидальные практики, участие в акциях, связанных с насилием и др.) через сеть Интернет.

Противоправная деятельность различных групп в сети Интернет вызывает особую тревогу, так как она приобретает значительные масштабы и вовлекает все большее количество менее защищенной категории населения – несовершеннолетних.

Интернет-среда на сегодняшний день является неотъемлемой частью жизни многих подростков. По данным Всероссийского центра изучения общественного мнения 89 % несовершеннолетних в возрасте от 14 до 17 лет и

53 % взрослых пользуются социальными сетями. Кроме того, 98 % несовершеннолетних и 69 % взрослого населения обозначили, что ежедневно используют сеть «Интернет» [13].

Соответственно, большая доля несовершеннолетних от 14 до 17 лет использует социальные сети и Интернет, что говорит о виртуализации их жизни и уязвимости при использовании сети «Интернет». Данную уязвимость (виктимность в некоторых случаях) используют представители криминальных структур для реализации преступных намерений, в том числе распространения запрещенной информации.

Подростковая среда в социальных сетях отмечается ростом количества несовершеннолетних, которые проявляют интерес к группам, продвигающим деструктивное поведение через темы нацизма, наркомании, массовых серийных убийств, обесценивания собственной жизни и приведения к смерти, а также экстремизма и радикализма [13].

В деструктивных идеях и движениях часто прослеживаются следующие цели:

- массовое и активное распространение деструктивной информации;
- обесценивание традиционных ценностей;
- деформация ценностей несовершеннолетних;
- формирование у несовершеннолетних ощущения неблагополучия и опасности в сети «Интернет» и в объективной реальности (состояние «тревожности» [14]);
- вербовка внушаемых и ориентированных на критику власти людей, устранения недовольства собственным положением для дальнейшего вывода их деструктивной активности в объективную реальность;
- дестабилизация социальной и политической обстановки государства.

Так, основными деструктивными течениями в социальных сетях являются:

- вовлечение в радикальные, в том числе террористические, организации;
- вовлечение в экстремистские организации, в том числе популяризирующие «идеологию насилия», нацизм, опасные субкультуры (скулшутеры, А.У.Е., ультрадвижение);
- околосуицидальные группы сообщества, пропагандирующие идеи обесценивания жизни, романтизирующие самоповреждения (селфхарм), содержащие сцены суицидальных действий или призывы к их совершению;
- мошенничество с помощью электронных средств платежа;
- незаконное распространение, в том числе хищение личных данных;
- троллинг, киберббулинг;
- деятельность по распространению и популяризации запрещенных химических веществ;
- сексуальное растление несовершеннолетних в сети «Интернет»;
- распространение компьютерных вирусов и т. д.

В настоящее время можно выделить следующие каналы распространения деструктивного контента:

1. Интернет-сайты, содержащие деструктивный контент и транслирующие его за счет публикации текстовой информации, фото-, видео- и аудиоматериалов. К сайтам также относятся и форумы, где напрямую можно встретить деструктивный контент, размещенный участниками беседы.

2. Социальные сети – в настоящее время основная платформа для публикации и трансляции деструктивного контента. Наиболее популярные социальные сети на территории РФ:

а) «ВКонтакте» (международное название VK) – российская социальная сеть со штаб-квартирой в Санкт-Петербурге, крупнейшая в Европе. Сайт доступен на многих языках, особенно популярен среди русскоязычных пользователей.

Распространение деструктивного контента в данной социальной сети возможно через аккаунты пользователей в социальной сети, как путем трансляции контента на своих персональных страницах (как самих сообщений, так и приглашений вступить в группу, пропагандирующую деструктивные идеи), так и популяризации деструктивных идей в частном общении (например, кураторы суицидальных игр или вербовщики).

Отдельным каналом распространения деструктивного контента становятся сообщества и информационные страницы в данной социальной сети, посвященные той или иной проблемной теме.

Отметим, что подача деструктивного контента в данных сообществах может идти как напрямую (призывы, утверждения), так и в завуалированной форме (приглашения в сообщества, популяризация идей и др.);

б) Facebook. Данный сайт входит в пятерку наиболее посещаемых вебсайтов мира. Facebook позволяет создать профиль с фотографией и информацией о себе, приглашать друзей, обмениваться с ними сообщениями, изменять свой статус, оставлять сообщения на своей и чужой «стенах», загружать фотографии и видеозаписи, создавать группы (сообщества по интересам).

Каналы распространения деструктивного контента аналогичны «ВКонтакте» – популяризация сообществ, прямо или косвенно пропагандирующих деструктивные идеи, частное общение, популяризация фото-, аудио- и видеоматериалов, содержащих деструктивный контент;

в) Instagram. В настоящее время Инстаграм становится достаточно новой площадкой для пропаганды деструктивного контента. Чаще всего им пользуются для распространения визуального материала (суицидальные мотиваторы, сцены насилия, постеры с призывами и др.);

г) Твиттер – деструктивный контент распространяется путем трансляции сообщений с заданным хештегом по той или иной теме;

д) Periscope – запрещенный контент распространяется зачастую в режиме реального времени, путем онлайн-трансляции (лекции, призывы и др.);

е) TikTok – ресурс для создания и распространения коротких мобильных клипов.

3. Глубокий Интернет (Глубокая паутина (также известна как «Невидимая сеть», «Глубокая сеть»; англ. DeepWeb)) – множество веб-страниц «Всемирной паутины», не индексируемых поисковыми системами. Наиболее значительной частью глубокой паутины является Глубинный веб (от англ. deepweb, hiddenweb), состоящий из веб-страниц, динамически генерируемых по запросам к онлайн-базам данных.

Главную опасность в сфере медиабезопаности представляет особый сегмент глубокого Интернета – Темный интернет (darknet) – сегмент глубокого Интернета, не индексируемый поисковыми машинами и не доступные через стандартные браузеры-сайты, в настоящий момент наиболее популярным способом подключения является Tor (TheOnionRouter) – программный сервис, анализирующий данные через множество собственных серверов и тем самым «заметающий» за пользователями все следы.

Благодаря почти полной анонимности и конспиративности темный Интернет становится все более популярным каналом распространения не только деструктивного контента, но и оборота нелегальных товаров и услуг (наркотики, порнография, оружие и пр.).

4. Электронная почта – каждый владелец электронной почты сталкивался с сомнительными рассылками, спамом, вирусами. Особую опасность с точки зрения медиабезопаности представляет собой незаконный доступ (взлом) к переписке со стороны третьих лиц.

5. Мессенджеры (IM, InstantMessenger) – это программа, мобильное приложение или веб-сервис для мгновенного обмена сообщениями. Наиболее популярные мессенджеры – WhatsApp, Viber, FacebookMessenger, Skype, ICQ, Telegram, Imessenger, Facetime и другие. С ростом популярности данного канала распространения информации мессенджеры начинают выполнять и другие функции, в частности посредством публичных каналов осуществляются функции СМИ. Благодаря функциям защиты переписки ряд мессенджеров становятся площадкой распространения деструктивного контента.

Деятельность деструктивных интернет-сообществ активно развивается, появляются новые направления и группы, которые негативно влияют на нормальное развитие детей и распространяют свою деятельность (деструктивный контент) по обширным современным каналам информации.

Вопросы для самоконтроля

1. Опираясь на прочитанный материал, сформулируйте собственное определение понятия «деструктивные интернет-сообщества».
2. Какие цели чаще всего прослеживаются в деструктивных течениях?
3. Назовите основные каналы распространения деструктивной информации в сети «Интернет».

Глава 3. Маркеры, характерные для проявления вовлечения несовершеннолетних в деятельность деструктивных интернет-сообществ

В 2020 г. Центр мониторинга социальных сетей (ГБУ ДПО «Челябинский институт развития профессионального образования») разработал перечень маркеров, характерных для проявления вовлечения несовершеннолетних в субкультуры деструктивной направленности по пяти актуальным для региона направлениям: 1) проявления околосуицидальных настроений; 2) популяризация субкультуры «колумбайн»; 3) развитие ультраправых взглядов; 4) уличная субкультура «оффников»; 5) вовлечение в радикальные организации [21].

Рассмотрим данные направления подробно.

1. Суицидальные настроения.

Вопросы пропаганды суицидального поведения в сети «Интернет» активно входят в новостную повестку последнего пятилетия, что связано с такими факторами, как [22]: 1) рост суицидальных актов среди детей и подростков; 2) развитие таких информационных каналов, как социальные интернет-сети, в которых «живут» дети и подростки (как в качестве пассивных – рядовых пользователей, так и активных – они являются администраторами собственных интернет-сообществ и др.); 3) появление моды на суицидальную и околосуицидальную тематику – практика селфхарма (самоповреждения путем нанесения порезов на вены и др.) в молодежной среде; тематика, связанная с вопросами суицидального поведения в литературе («50 дней до моего самоубийства»), молодежных сериалах («13 причин "почему"») и др.; 4) громкое освещение темы суицидального поведения и пропаганды суицидального поведения в СМИ, как в контексте совершившихся актов («эффект Вертера»), так и мифологизации данных проблем (например, тема появления «игр смерти» в социальных интернет-сетях) и др.

При этом, говоря о пропаганде суицидального поведения в социальных сетях Интернета и в целом в интернет-пространстве, следует отметить, что данные каналы и механизмы являются вторичными причинами суицидальных действий детей и подростков, при этом первопричинами остаются традиционные для данной категории проблемы, такие как: сложности во взаимоотношениях с окружающими (одноклассниками, учителями, семьей), безответная любовь, депрессия и психологические (психиатрические) проблемы, экономические факторы и др.

Следовательно своевременное выявление интернет-профилей учащихся, находящихся в «группе риска», осуществление комплексной работы психолога и педагога с ними (включающей, в том числе и элементы ресоциализации) позволят не допустить распространение потенциальных угроз и вовлечение в них, как по отношению учащегося к самому себе (реализации суицидальных идей), так и к обществу в целом (случаи школьного шутинга, буллинга и др.).

В анализе проблем, связанных с интересом детей и подростков к суицидальным практикам, следует обращать внимание на совокупность следующих маркеров:

1. Визуальные маркеры:

– изменение стиля: преимущественно закрытая одежда (попытка скрыть руки);

– порезы на руках, бедрах, ссадины.

2. Виртуальные маркеры:

– публикация депрессивных статусов;

– подписка на сообщества, содержащие околосуицидальный контент, в том числе контент, романтизирующий смерть, одиночество, депрессию, самоповреждение (от анорексии до селфхарма) и др.

3. Вербальные маркеры:

– высказывание желания умереть;

– вербальные угрозы совершить самоубийство;

– позитивная оценка суицидальных практик и др.;

– употребление специфического сленга: «выпилиться», «обнулиться», «самовыпил» и др.

4. Эмоциональные маркеры:

– смена эмоционального поля (жизнерадостный подросток вдруг стал замкнутым).

Дополнительные факторы:

– наличие проблем в семье (внутрисемейные конфликты, развод родителей, смерть одного из близких родственников и др.);

– неразделенная любовь (расставание, чувство «отверженности»);

– в прошлом наличие попыток совершения самоубийства (суициды близких людей);

– наличие кумира, совершившего самоубийство (Курт Кобейн, LilPeep, Честер Беннинктон и др.).

2. Популяризация культуры скулшутеров.

Скулшутинг – это вооруженное нападение внутри учебного заведения.

Среди обязательных условий, характеризующих совершение скулшутинга:

а) совершение преступлений в организациях системы образования;

б) отсутствие требований к личности преступника (вне зависимости от пола, возраста, социальных характеристик, в том числе принадлежности к конкретной образовательной организации);

в) направленность умысла преступника на причинение вреда жизни и (или) здоровью неограниченного круга лиц;

г) применение в качестве орудия совершения преступлений стрелкового оружия и/или взрывных устройств.

В анализе проблем, связанных с интересом детей и подростков к идеям скулшутинга следует обращать внимание на совокупность следующих маркеров:

1. Визуальные маркеры:

– изменение стиля одежды: черный длинный плащ, черные штаны с большим количеством карманов, высокие ботинки;

– белая футболка с характерной надписью («Ярость», «Ненависть», «Естественный отбор», «KMFDM» как на русском, так и иностранных языках) и др.

2. Виртуальные маркеры:

– подписка на сообщества, романтизирующие субкультуру «колумбайн»;

– публикация визуальных изображений скулшутеров (Эрика Харриса, Дилана Клиболда, Влада Рослякова и др.);

– статусы, содержащие цитаты из дневников скулшутеров или оправдывающие насилие (расстрелы, взрывы) в образовательном учреждении.

3. Вербальные маркеры:

– упоминание имен скулшутеров (Эрик Харрис, Дилан Клиболд, Влад Росляков и др.);

– оправдание поступков скулшутеров, высказывания о подготовке к собственному «колумбайну» и др.

4. Эмоциональные маркеры:

– смена эмоционального поля (жизнерадостный подросток вдруг стал замкнутым).

Словарь «скулшутера»:

1) «Колумбайн» – массовое убийство в школе «Колумбайн», спланированное нападение двух учеников старших классов школы «Колумбайн» округа Джефферсон, штат Колорадо, Эрика Харриса и Дилана Клиболда на остальных учеников и персонал этой школы, совершенное 20 апреля 1999 г. с применением стрелкового оружия и самодельных взрывных устройств;

2) Эрик Харрис и Дилан Клиболд – два ученика старших классов, которые устроили массовое убийство в школе «Колумбайн»;

3) «NBK» – «NaturalBornKillers» – название картины Оливера Стоуна «Прирожденные убийцы» на английском языке. Аббревиатурой «NBK» Эрик Харрис и Дилан Клиболд назвали день нападения на школу;

4) «ПУ» – аббревиатура отсылает к фильму «Прирожденные убийцы». Этой аббревиатурой Эрик Харрис и Дилан Клиболд обозначали предстоящее массовое убийство;

5) «Водка» («Vodka») – один из псевдонимов Дилана Клиболда в Интернете;

6) «Reb» – сокращенно от «Мятежник» (англ. «Rebel») – один из псевдонимов Эрика Харриса в Интернете;

7) «Джоки» – отсылка к сленговому обозначению спортсменов, которым пользовались Эрик Харрис и Дилан Клиболд;

8) «KMFDM» – грамматически неверный акроним названия немецкой музыкальной группы «KeinMehrheitFür Die Mitleid». Тексты некоторых песен

«KMFDM» – «Sonof a Gun», «StrayBullet», «Waste» – были размещены на личной странице Эрика Харриса, одного из убийц школьников;

9) «Naturalselection» – в день совершения массового убийства в школе «Колумбайн» на одном из убийц была надета белая футболка с данной надписью черными буквами;

10)«Wrath» («гнев») – в день совершения массового убийства в школе «Колумбайн» на одном из убийц была надета белая футболка с данной надписью черными буквами.

3. Проблемы распространения ультраправой идеологии.

В анализе проблем, связанных с интересом детей и подростков к идеологии ультраправых, следует обращать внимание на совокупность следующих маркеров:

1. Визуальные маркеры:

– визуальное отображение на одежде следующей символики: цифры 88 и 18 (88-HH) это аббревиатура, обозначающая HeilHitler, а 18 – AH – AdolfHitler);

– преобладание одежды следующих брендов: ThorSteinar, «Белояр»,«SVA STONE», «Своя культура».

2. Виртуальные маркеры:

– публикация статусов, критикующих и оскорбляющих других людей по признаку национальности, религии, социального статуса (например, мигранты);

– подписки на сообщества, содержащие упоминания «ультра», «ультраправые», «белая раса» и др., а также контент, содержащий оправдание действий и романтизацию поступков националистов.

3. Вербальные маркеры:

– высказывание презрения к лицам, принадлежащим к «не русской» национальности;

– критика дружбы и любых других отношений с представителями «нерусской» национальности;

– унижение, оскорбление других людей по признаку их религии или национальности.

Словарь ультранационалиста:

1) «4/20» – годовщина со дня рождения Адольфа Гитлера, также используется в качестве тату расистов и неонацистов, чтобы подтвердить свою веру в идеалы национал-социализма. Общей, но совершенно другой смысл для «4/20» (или «4:20» или «420») является, как сленговый термин, связанный с курением марихуаны;

2) «Зиг хайль!» (нем. SiegHeil! – «Да здравствует победа!» или «Слава победе!») – «88» – лозунг, употреблявшийся на собраниях и митингах Национал-социалистической немецкой партии;

3) A. C. A. B. – (англ. allcopsarebastards) (оскорб.) – «12/13» – «все полицейские – ублюдки»;

4) «За Русь великую!» – лозунг «За Русь великую!!!!» активно используется в различных группах, придерживающих националистической и национал-социалистической идеологии;

5) «18» – означает первую и восьмую буквы алфавита = АН = Adolf Hitler. Число можно видеть, например, в названии английской неонацистской группы «Комбат 18» (Combat18);

6) «88» – Числовой акроним клича «HeilHitler!»;

7) «8» – позиция буквы «Н» в латинском алфавите;

8) «14» – код известных «14 слов» американского неонациста Дэвида Лейна («Мы должны оберегать существование нашего народа и будущее для наших белых детей» – «Wemust secure the existence of our people and the future for our white children»). «14 слов» – одна из основных фраз сегодняшней неонацистской идеологии. Часто комбинируется с «88», например «14/88»;

9) «14/18» – кодовая фраза и надпись на заборах – плод воображения американского националиста Дэвида Лэйна. Цифра «14» совпадает с количеством слов в его лозунге о сохранении белого народа, а «88» связана с приветствием «HeilHitler!» (буква «Н» стоит в латинском алфавите восьмой).

4. Проблема вовлечения детей и подростков в радикальные религиозные организации.

Маркеры увлечения учащихся идеологией радикальных религиозных организаций:

1. Визуальные маркеры:

– для девушек – резкое изменение стиля одежды: «покрытие» головы – ношение «хиджаба».

2. Виртуальные маркеры:

– публикация статусов религиозного содержания (символика, религиозные цитаты и др.).

3. Вербальные маркеры:

– деление людей на «истинных» и «неверных»;

– упоминание в разговоре религиозных догматов, эсхатологические высказываний (ожидание конца света);

– цитирование духовных учителей, гуру, проповедников, озвучивание планов уехать из страны.

4. Эмоциональные маркеры:

– смена эмоционального поля (жизнерадостный подросток вдруг стал замкнутым).

Дополнительно:

– непризнание органов государственных власти, традиционных религиозных институтов, государственных праздников;

– внезапное обостренное внимание к международной обстановке.

5. Уличные околокриминальные субкультуры.

Маркеры увлечения учащихся субкультурой «оффников»:

1. Визуальные маркеры:

– вещи с логотипами «Supreme», «Palace», «THRASHER», «TommyHilfiger», футболки фирмы «Спутник 1985», камуфляжные штаны (куртки), куртки со значком компаса, вещи с лейблом «NAPAPIJRI» и «The North Face», нашивки «Stone Island», кроссовки «New Balance», «Nike».

Часто «оффник», видящий другого подростка в такой же одежде, ищет причины для самоутверждения и драки – «предъявляет за шмот».

2. Виртуальные маркеры:

– наличие в подписках сообществ, популяризирующих криминальные или уличные субкультуры «АУЕ», «оффники», «забивы», «хулиганы», «лесные танцоры» и др.

3. Вербальные маркеры:

– использование специфического сленга («брат за брата», «жизнь – ворам», «АУЕ» и др.),

– приглашение к участию в «забивах», сходках и др.

Словарь уличной молодежной субкультуры «оффников».

Оффники – молодежное движение, сеть разрозненных сообществ по всей России, состоящих из подростков от 12 до 18 лет, подражающих околофутбольным фанатам 1990-х. Данная субкультура сейчас популярна среди подростков, имеет свои внешние проявления и внутригрупповые ценности.

Поляна – драка в лесу подальше от чужих глаз поздно вечером.

Забив – групповая драка, происходящая на договорных встречах (аналог «стрелок»). Зачастую «забивы» снимаются на телефон с последующей трансляцией в Интернет.

Лесная принцесса – лидер команды оффников.

Лесной танцор – оффник, участвующий в забиве.

Лес – место для забивов. Часть культа оффника.

Черт – жертва оффников, намеченная предварительно и приглашенная на забив. Есть мнение, что о своем статусе «черта» человек может и не знать.

Важно, что в некоторых объединениях «оффников» при проигрыше в «забиве» проигравший отдает часть своей одежды и телефон победителю.

Лидеры команд оффников никогда не дерутся, они решают, сколько участников будет в «забиве», когда остановиться, также часто ведут видеосъемку «забива» и «отбива» «черта». Избиение идет, пока лидер не скажет «стоп», или пока жертва избиения не потеряет сознание.

Соответственно, рассматривая вопросы выявления противоправной деятельности деструктивных интернет-сообществ и их виды, необходимо в первую очередь понимать значимость установления причин и условий, способствующих указанной противоправной деятельности, и проведения эффективных, комплексных предупредительных мероприятий, которые направлены на выстраивание комплексной профилактической работы.

Представленная структура маркеров увлечения несовершеннолетних суицидальными практиками; субкультурой «колумбайн»; ультраправовой идео-

логией; идеологией радикальных религиозных организаций; субкультурой «оффников» позволит субъектам профилактики принимать своевременные меры, вместе с тем комплексное воздействие мер на несовершеннолетних может быть реализовано только посредством привлечения такого института как семья.

В этой связи в семье следует обращать особое внимание на поведенческие особенности несовершеннолетних, что в объективной реальности проявляется следующим образом:

1. Изменилась манера поведения несовершеннолетнего на более грубую, агрессивную, а также доминирует раздражительность к окружающим.
2. В речи несовершеннолетнего прогрессирует ненормативная и жаргонная лексика.
3. Увлеченность вредными привычками и занятием противоправной деятельностью (алкоголизм, наркомания, курение и т. д.).
4. Изменился стиль одежды – ношение одежды с нетипичной символикой, атрибутикой, которая относится к определенной субкультуре (например, нацистская символика, нанесение татуировок и т. д.).
5. На компьютере оказывается много сохраненных ссылок или файлов с текстами, роликами или изображениями экстремистко-политического или социально-экстремального содержания, а также суицидального содержания.
6. Снижение успеваемости, систематические прогулы учебных занятий в школе.

В связи с этим субъектам профилактики при общении с детьми необходимо быть особенно внимательными к внутреннему миру и чувствам несовершеннолетних в подростковый период, строить с ними доверительные отношения, поскольку незначительный, с точки зрения взрослого, повод может повлечь за собой деструктивные последствия в виде суицида, совершения преступления, правонарушения.

Соответственно, можно выделить следующие маркеры определения поведенческих признаков несовершеннолетних, вовлеченных в деструктивные Интернет-сообщества: маркеры увлечения несовершеннолетних суицидальными практиками, субкультурой «колумбайн», ультраправовой идеологией, идеологией радикальных религиозных организаций, субкультурой «оффников». В практической деятельности субъектов профилактики правонарушений маркеры позволят на ранних стадиях предупредить противоправную деятельность деструктивных интернет-сообществ и оптимизировать работу. При этом родителям следует уделять внимание на поведенческие признаки характерных несовершеннолетним, вовлеченных в деятельность деструктивных интернет-сообществ.

Вопросы для самоконтроля

1. Проанализируйте параграф и раскройте особенности поведенческих маркеров «группы риска».
2. Перечислите основные направления поведенческих маркеров «группы риска».
3. Назовите, какие поведенческие особенности проявляются у несовершеннолетних, вовлеченных в деструктивные интернет-сообщества.

Глава 4. Деятельность органов внутренних дел по предупреждению вовлечения несовершеннолетних в деятельность деструктивных интернет-сообществ

В настоящее время существенной проблемой обеспечения общественной безопасности становятся объективно не мотивированные вспышки насилия в подростковой среде. Они носят разнообразный характер – массовые драки, насилие одного субъекта по отношению к группе, насилие со стороны группы над одним субъектом, межиндивидуальное насилие и т. п. [23]

Насилие среди несовершеннолетних приводит к серьезному стрессу, который связан с нарушением раннего развития мозга детей. По данным исследований, опубликованным в 2020 г. Всемирной организацией здравоохранения, экстремальный стресс может нарушать развитие нервной и иммунной систем несовершеннолетних [20]. Вследствие этого в зрелом возрасте людям, подвергавшимся насилию в детстве, угрожает повышенный риск возникновения проблем в области поведения, физического и психического здоровья, таких как:

- совершение насилия или становление жертвой насилия;
- депрессия;
- курение;
- ожирение;
- незапланированная беременность;
- злоупотребление алкоголем и наркотиками;
- сексуальное поведение.

Известно, что подростки подвержены формированию установок на агрессивное поведение, дополнительную опасность для них несут [23]:

1) возможность целенаправленной пропаганды экстремального поведения в Интернете;

2) разжигание агрессии посредством экстремистских лозунгов;

3) политизация социально-экономических проблем;

4) романтизация образов «отрицательных героев» (Эрик Харрис, Дилан Клиболд, Филипп Лис, лидеры экстремистских и террористических организаций и др.);

5) навязывание подросткам идей, пропагандирующих насилие в качестве социальной нормы путем погружения их в деструктивные интернет-сообщества.

Ряд социальных и политических организаций занимается сегодня целенаправленным формированием «культуры насилия» в подростковой среде.

«Культура насилия» характеризуется следующими чертами [23]:

– насилие рассматривается как не просто допустимый, а поощряемый и самоценный вид деятельности;

– культ силы, лидерства (вождизма), авторитарного характера;

– культ группы, сплоченности, единства (пренебрежение мнением члена группы);

– любые проявления инаковости, несогласия, слабости воспринимаются в качестве причины для применения насилия;

– публичные проявление агрессивности рассматриваются как желательные;

– цель насилия может иметь вторичную значимость;

– размер общественного ущерба не имеет значения.

Наибольший эффект по предупреждению асоциального поведения несовершеннолетних может быть достигнут лишь совместными усилиям всех субъектов системы профилактики.

Комплексная работа родителей, педагогов, психологов и сотрудников полиции по формированию и развитию семейных, патриотических, нравственных, религиозных, философских ценностей (любви, дружбы, взаимопомощи и взаимовыручки, взаимоуважения) у ребенка должна осуществляться с самого раннего возраста.

Соответственно, для своевременного выявления и предупреждения вовлечения несовершеннолетних в противоправную деятельность деструктивных интернет-сообществ, как мы полагаем, следует выделять эффективные меры предупреждения, которые могут быть применены сотрудниками правоохранительных органов.

1. Профилактическая работа с несовершеннолетними, находящимися в группе риска, потенциально способными приобщиться к деструктивным молодежным движениям. Она должна сводиться к формированию такого сценария поведения, при котором несовершеннолетний почувствует себя значимым для общества и для общего дела.

В этой связи необходимо переориентировать «потенциально опасных» подростков на позитивную деятельность (особенно более виктимную категорию в возрасте 14–16 лет). Важно сформировать внутреннее убеждение в том, что поставленные перед ними цели и задачи являются их собственными, а достижение и решение этих задач отвечает их будущим интересам.

2. Осуществление обмена информацией между субъектами профилактики. Сотрудникам полиции необходимо постоянно поддерживать контакт с социальными педагогами и психологами с целью обмена информацией о поведении несовершеннолетних и степени социально-психологического благополучия интересующей группы. Необходимо получать информацию о лицах,

пропагандирующих девиантное поведение, а также причисляющих себя к неформальным молодежным объединениям деструктивной направленности.

3. Профилактическая работа с законными представителями несовершеннолетних. Проводить профилактическую работу необходимо не только среди учеников, но и с их родителями. Необходимо разъяснять им признаки негативного влияния асоциальных групп на личность подростка (недоверие, агрессивное поведение, эмоциональный дискомфорт, непринятие себя), способы вовлечения несовершеннолетних в данные группы, указывать на необходимость контроля круга общения своего ребенка, как в реальной жизни, так и в социальных сетях.

Таким образом, главная задача совместных усилий сотрудников полиции, социальных педагогов, психологов и родителей должна состоять в доведении до подростка необходимости сопротивляться негативному влиянию СМИ, «друзей и товарищей», идеализирующих асоциальное поведение.

4. Мониторинг сети «Интернет» на предмет выявления деструктивных интренет-сообществ, которые осуществляют вовлечение несовершеннолетних в свою противоправную деятельность.

Сотрудниками ОВД проводятся оперативно-розыскные мероприятия, направленные на выявление, пресечение и раскрытие преступлений, связанных с деятельностью лиц, вовлекающих несовершеннолетних в деструктивные интернет-сообщества посредством использования сети «Интернет» и социальных сетей.

При осуществлении анализа и мониторинга страниц несовершеннолетних в социальных сетях, необходимо обращать внимание на следующие признаки:

– *адрес аккауната, имя аккаунта.*

В частности несовершеннолетние, вовлеченные в деятельность деструктивных интернет-сообществ, используют такие наименования в названии своего аккаунта, как «смерть», «ангел одиночества», «ангел зла», имена персонажей суицидальных игр, лидеров агрессивных движений и др. Вместо своих актуальных и реальных данных, несовершеннолетние указывают псевдонимы, а именно используют имена различных криминальных авторитетов, лидеров криминальных субкультур;

– *количество друзей и подписчиков.*

В большинстве случаев на аккаунте у подростка имеется небольшое количество подписчиков и друзей, характерной особенностью которых является пропаганда экстремизма, насилия, суицида;

– *сообщества, на которые подписан подросток в социальных сетях.*

Подросток подписан на сообщества, пропагандирующие суицидальный или насильственный контент (депрессивные статусы, суицидальные игры, культ оружия, призывы к насилию в школе);

– *география или местоположение.*

Данную графу в социальных сетях несовершеннолетние не заполняют либо указывают другие страны, города – например, Япония (Токио), Канада, Германия и др.;

– *фотографии.*

Изображения лидеров криминальных субкультур, использование изображений депрессивной тематики, размещение фотографии людей с оружием и т. д.;

– *записи, «хэштэги», размещенные на странице в социальной сети.*

Страница полностью очищена; размещен контент депрессивного (проблемы отсутствия понимания, любви, селфхарм (порезы на венах) и др.) или агрессивного характера (оружие, призывы к агрессии, видео терактов, казней и др.);

– *время активности в социальных сетях.*

Данные аккаунты несовершеннолетних активны в ночное время.

Также в рамках мониторинга сети Интернет на предмет выявления деструктивных Интернет-сообществ необходимо тесно взаимодействовать с Роскомнадзором и Роспотребнадзором, поскольку данные ведомства занимаются непосредственно выявлением деструктивных интернет-сообществ и техническим блокированием (подробно рассмотрено в главе 5).

5. *Информационная просветительская деятельность.*

Сотрудникам ОВД необходимо проводить в образовательных организациях профилактические беседы в форме лекций, бесед и тематических выступлений, которые, соответственно, будут направлены на безопасное использование сети «Интернет», с разъяснением пагубности влияния деструктивных интернет-сообществ. В рамках проведения профилактических бесед необходимо распространять памятки для родителей, педагогов и несовершеннолетних о безопасном использовании интернет-пространства.

При проведении тематических бесед необходимо также доводить информацию о порядке обращения за помощью в территориальные органы МВД России при обнаружении признаков вовлечения несовершеннолетних в деструктивные интернет-сообщества, а также в медицинские организации и в другие органы системы профилактики.

Кроме того, необходимо организовать и проводить различные викторины, конкурсы, интеллектуальные игры, конференции и другие мероприятия, которые будут направлены на формирование навыков и умений у несовершеннолетних безопасного использования сети «Интернет». Проведение данных мероприятий позволит осветить проблемы интернет-зависимости у детей, довести информацию о негативном влиянии деструктивных интернет-сообществ и о способах защиты в интернет-среде от них.

Также необходимо внедрять и развивать «горячие линии» или «телефон доверия», то есть консультативно-психологическую помощь несовершеннолетним, которая будет работать в круглосуточном режиме в случае возникновения трудной жизненной ситуации.

Важным звеном профилактики является взаимодействие с молодежными организациями, волонтерами и общественными организациями правоохранительной направленности в рамках предупреждения вовлечения несовершеннолетних в деструктивные интернет-сообщества.

Согласно официально опубликованным данным ГУОООП МВД России, в настоящее время в сети «Интернет» имеется свыше 200 сайтов, на которых общественными организациями, молодежными блогерами и гражданами с активной жизненной позицией при поддержке региональных органов исполнительной власти размещается информация для несовершеннолетних и родителей [19].

Так, например, МВД России в рамках взаимодействия с общественными организациями, такими как: Всероссийская общественная организация «Молодая гвардия Единой России», «Лига Безопасного Интернета», АНО «Интернациональный центр спасения детей от киберпреступлений», осуществляется анализ страниц подростков социальных сетей в сети «Интернет».

Также необходимо оказывать помощь в организации деятельности общественных объединений правоохранительной направленности и тесно взаимодействовать с такими молодежными объединениями, как «Юные помощники полиции», «Детская кибердружина», «Родительское собрание».

Соответственно, сотрудникам ОВД необходимо своевременно выявлять факты вовлечения несовершеннолетних в деструктивные интернет-сообщества, а также осуществлять комплексную профилактическую работу с ними, посредством реализации следующих мер:

– профилактическая работа с несовершеннолетними, находящимися в группе риска, потенциально способными приобщиться к деструктивным молодежным движениям;

– осуществление обмена информацией между субъектами профилактики;

– профилактическая работа с законными представителями несовершеннолетних;

– мониторинг сети «Интернет» на предмет выявления деструктивных интренет-сообществ, которые осуществляют вовлечение несовершеннолетних в свою противоправную деятельность;

– информационная-просветительская деятельность.

Вопросы для самоконтроля

1. Перечислите основные направления деятельности органов внутренних дел по предупреждению вовлечения несовершеннолетних в деятельность деструктивных интернет-сообществ.

2. Назовите характерные признаки для осуществления интернет-мониторинга страниц в социальных сетях на предмет выявления вовлеченности несовершеннолетних в деструктивные интренет-сообщества.

3. Как осуществляется взаимодействие МВД России с общественными организациями по предупреждению вовлечения несовершеннолетних в деструктивные интернет-сообщества?

Глава 5. Алгоритм интернет-мониторинга на предмет выявления деятельности деструктивных интернет-сообществ и процедура блокировки сайтов и сообществ, содержащих запрещенную информацию

В настоящее время в интернет-пространстве существуют социальные сети, мессенджеры, информационные сайты, где может распространяться информация, носящая деструктивный характер, и их количество имеет тенденцию к росту. Поэтому актуальность выработки алгоритма интернет-мониторинга на предмет выявления деятельности деструктивных интернет-сообществ приобретает особую значимость.

Необходимость своевременного выявления деятельности деструктивных интернет-сообществ, выработка определенного алгоритма поиска, пресечение их деятельности позволят не допустить потенциальных угроз негативного воздействия на граждан, а также совершения противоправных действий в результате такого отрицательного воздействия.

Постоянный интернет-мониторинг на предмет выявления деятельности деструктивных интернет-сообществ необходимо осуществлять ежедневно силами сотрудников правоохранительных органов, в том числе сотрудников органов внутренних дел, что позволит минимизировать возможность вовлечения детей в деятельность деструктивных интернет-сообществ и распространения негативной информации.

Интернет-мониторинг заключается в следующем:

1. Анализ с помощью поисковых систем (Google, Yandex, Mail.ru, Yahoo, Bing) соответствующих ключевых слов, которые могут быть связаны с деятельностью деструктивных интернет-сообществ.

2. Просмотр молодежных форумов, подростковых сайтов, где наиболее вероятно происходит обсуждение информации, носящей деструктивных характер для несовершеннолетних. Особенности мониторинга в данном случае будут заключаться в осуществлении поиска на странице сайта с помощью сочетания клавиш на клавиатуре CTRL+F и введения соответствующих ключевых слов.

3. Мониторинг социальных сетей ВКонтакте, Одноклассники, Telegram, Facebook, Instagram в целях установления групп, которые могут включать информацию, несущую деструктивный характер – необходимо осуществить определенную выборку по их наименованию. Для этого необходимо в строке поиска сообществ ввести наиболее характерные слова либо словосочетания, подпадающие под деятельность деструктивных сообществ, такие как «оружие», «наркотики», «суицид», «вписки», «изготовление взрывчатки», «А.У.Е.», «смерть мусорам, свободу ворам» и т. п.

Отталкиваясь от полученных результатов поиска, необходимо проверить данные сообщества на предмет наличия в них различного рода призывов совершать определенные действия, носящие антиобщественный или аморальный характер. Далее следует проверить аудио- и видеозаписи, которые были

«прикреплены» в сообществе, группе на предмет наличия информации, указанной выше.

В случае установления наличия в группах информации, носящей деструктивный характер, следует подготовить обращение в Роскомнадзор для того, чтобы данное сообщество было заблокировано.

Процедура блокировки запрещенной информации регламентирована законодательством Российской Федерации.

Так, согласно ст. 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» [4] существует Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено (далее – Реестр), который ведется в целях ограничения доступа к сайтам сети «Интернет», содержащим запрещенную информацию.

К запрещенной информации в соответствии с Реестром относится информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий [3]. Сайты и сообщества социальных сетей, содержащие в себе указанную запрещенную информацию, вносятся в Реестр.

Основаниями для включения в Реестр сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие запрещенную информацию, являются:

– решения уполномоченных федеральных органов исполнительной власти: Министерства внутренних дел Российской Федерации (далее – МВД России), Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека (далее – Роспотребнадзор), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор), Федеральная служба по надзору в сфере здравоохранения (далее – Росздравнадзор), Федеральная налоговая служба, Федеральная служба по регулированию алкогольного рынка (далее – Росалкогольрегулирование), Федеральное агентство по делам молодежи (далее – Росмолодежь);

– вступившее в законную силу решение суда о признании информации, распространяемой посредством сети «Интернет», запрещенной;

– постановление судебного пристава-исполнителя об ограничении доступа к информации, распространяемой в сети «Интернет», порочащей честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического лица.

Особенности процедуры блокировки сайтов и сообществ, содержащих запрещенную информацию, регламентируются ст. 15.1 Федерального закона от

27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» [4], а также Постановлением Правительства РФ от 26 октября 2012 г. № 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» [10].

Решение о внесении в Реестр сайтов и сообществ, содержащих запрещенную информацию, принимается Роскомнадзором.

Роскомнадзор размещает на своем официальном сайте в сети «Интернет» в электронном виде форму для приема обращений органов государственной власти и органов местного самоуправления, юридических лиц, индивидуальных предпринимателей, общественных объединений и иных некоммерческих организаций, а также граждан о наличии на страницах сайтов в сети «Интернет» запрещенной информации в целях взаимодействия с указанными органами власти, физическими и юридическими лицами в рамках деятельности по формированию и ведению единого Реестра [10].

Направление материала на блокировку можно осуществлять через электронную форму приема обращений граждан и юридических лиц по вопросам функционирования Единого реестра доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено. Для этого необходимо выбрать пункт «выявлена противоправная информация», а далее – вид данной информации (признаки призыва к самоубийству, вовлечения несовершеннолетних к противоправным действия и др.).

После поступления обращения в Роскомнадзор и (или) оператору Реестра в течение суток запрос с названием указателя страницы сайта в сети «Интернет» о возможном наличии на указанной странице сайта запрещенной информации направляется в электронном виде (в рамках системы взаимодействия) уполномоченным органам в соответствии с их компетенцией [10]:

1. МВД России – в отношении распространяемой посредством сети «Интернет» информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, а также о способах и местах культивирования наркосодержащих растений;

2. Роспотребнадзор – в отношении распространяемой посредством сети «Интернет» информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

3. Роскомнадзор – в отношении: материалов с порнографическими изображениями несовершеннолетних, объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера, распространяемых посредством сети «Интер-

нет»; информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, о способах и местах культивирования наркосодержащих растений и о способах совершения самоубийства, призывов к совершению самоубийства, размещенной в продукции средств массовой информации, распространяемой посредством сети «Интернет»; информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами, размещенной в продукции средств массовой информации, распространяемой посредством сети «Интернет»; информации, распространяемой посредством сети «Интернет», решение о запрете к распространению которой на территории Российской Федерации принято уполномоченными органами или судом;

4. Росздравнадзор – в отношении распространяемой посредством сети «Интернет» информации, содержащей предложение о розничной торговле лекарственными препаратами для медицинского применения, в том числе дистанционным способом, розничная торговля которыми ограничена или запрещена в соответствии с законодательством Российской Федерации;

5. Федеральная налоговая служба – в отношении распространяемой посредством сети «Интернет» информации об организации и проведении азартных игр и лотерей с использованием сети «Интернет» и иных средств связи;

6. Росалкогольрегулирование – в отношении распространяемой посредством сети «Интернет» информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, спиртосодержащей пищевой продукции, этилового спирта, спиртосодержащей непищевой продукции, розничная продажа которых ограничена или запрещена законодательством Российской Федерации;

7. Росмолодежь – в отношении распространяемой посредством сети «Интернет» информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц, а также информацию о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами.

После обработки и проверки информации по запросу Роскомнадзора вышеуказанные уполномоченные федеральные органы исполнительной власти предоставляют информацию о решении, принятом по запросу в Роскомнадзор и (или) оператору Реестра в электронном виде (в рамках системы взаимодействия) в течение суток после получения такого запроса, а при необходимости проведения экспертизы – в течение 7 суток после получения такого запроса.

Данное решение должно содержать следующие сведения:

– наименование уполномоченного органа, принявшего решение;

– номер принятого решения, дата и время его принятия;

– фамилия, имя, отчество и должность должностного лица (лиц), принявшего решение о наличии на странице сайта в сети «Интернет» запрещенной информации;

– доменное имя и (или) указатель страницы сайта в сети «Интернет», содержащего информацию или материалы, в отношении которых принято соответствующее решение;

– описание выявленной запрещенной информации, позволяющее ее идентифицировать, включая (если имеется) ее название, с приложением копии страницы сайта в сети «Интернет», заверенной усиленной квалифицированной электронной подписью должностного лица уполномоченного органа.

Далее уполномоченный сотрудник Роскомнадзора и (или) оператор Реестра осуществляет техническую блокировку сайтов и сообществ, содержащую запрещенную информацию. Процедура блокировки сайтов и сообществ следующая:

1. Оператор Реестра (организация, привлекаемая Роскомнадзором к ведению Реестра) уведомляет провайдера хостинга о намерении включить доменное имя и (или) указателя страницы сайта в Реестр.

2. Провайдер хостинга обязан проинформировать об этом обслуживаемого им владельца сайта и уведомить о необходимости незамедлительно удалить интернет-страницу с запрещенной информацией.

3. Владелец сайта в течение суток обязан удалить интернет-страницу, в противном случае провайдер хостинга обязан ограничить доступ к такому сайту.

Таким образом, одним из направлений деятельности Роскомнадзора является блокировка сайтов и сообществ в сети «Интернет», содержащих запрещенную информацию. Также Роскомнадзор в рамках межведомственного взаимодействия активно сотрудничает с органами внутренних дел по оперативному обмену информацией о сообществах и группах, пропагандирующих и призывающих несовершеннолетних к насилию, убийству, агрессии через посредство информационно-коммуникационной сети «Интернет», что позволяет минимизировать факты вовлечения несовершеннолетних в деструктивные интернет-сообщества.

Вопросы для самоконтроля

1. Определите, в чем заключается интернет-мониторинг на предмет выявления деятельности деструктивных интренет-сообществ.

2. Раскройте процедуру блокировки сайтов и сообществ, содержащие запрещенную информацию.

3. Назовите основания для включения в единый реестр доменных имен и (или) указателей страниц сайтов в сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие запрещенную информацию.

Заключение

На основании проведенного нами исследования можно сделать следующие выводы.

Стоит отметить, что если деятельность официальных медиа регламентируется и контролируется на законодательном уровне, то неофициальные информационные источники, распространяющиеся в сети «Интернет» информацию посредством социальных сетей (аккаунтов, сообществ), не поддаются контролю за счет своей стихийности и массовости, тем самым имея возможность активно распространять и пропагандировать деструктивный контент среди пользователей Интернета.

Для своевременного выявления и предупреждения вовлечения несовершеннолетних в противоправную деятельность деструктивных интернет-сообществ разработаны эффективные меры предупреждения, такие как: мониторинг сети «Интернет», а именно популярных среди молодежи социальных сетей; ведение сотрудниками органов внутренних дел информационно-просветительской деятельности; осуществление комплексной работы в рамках взаимодействия с молодежными организациями, волонтерами и общественными организациями правоохранительной направленности, а также с психолого-медико-педагогическими комиссиями. Данные меры предупреждения позволят предупредить и не допустить негативные последствия как для самого подростка (например, реализации суицидальных идей), так и общества в целом (акций школьного шутинга, буллинга и др.).

Маркеры определения поведенческих признаков несовершеннолетних, вовлеченных в деструктивные интернет-сообщества – это маркеры увлечения несовершеннолетних суицидальными практиками, субкультурой «колумбайн», ультраправовой идеологией, идеологией радикальных религиозных организаций, субкультурой «оффников». В практической деятельности субъектов профилактики правонарушений маркеры позволят на ранних стадиях предупредить противоправную деятельность деструктивных интернет-сообществ и оптимизировать работу. При этом родителям следует уделять внимание выявлению поведенческих признаков, характерных для несовершеннолетних, вовлеченных в деятельность деструктивных интернет-сообществ.

Выработанный алгоритм постоянного интернет-мониторинга на предмет выявления деятельности деструктивных интернет-сообществ позволит органам внутренних дел не допустить потенциальных угроз негативного воздействия на несовершеннолетних.

Таким образом, одним из направлений деятельности Роскомнадзора является блокировка сайтов и сообществ в сети «Интернет», содержащих запрещенную информацию. Также Роскомнадзор в рамках межведомственного взаимодействия активно сотрудничают с органами внутренних дел по оперативному обмену информацией о сообществах и группах, пропагандирующих

и призывающих несовершеннолетних к насилию, убийству, агрессии через посредство информационно-коммуникационной сети «Интернет», что позволяет минимизировать факты вовлечения несовершеннолетних в деструктивные интернет-сообщества.

Учитывая развитие информационно-телекоммуникационной сети «Интернет» и использование указанной сети обширным количеством людей, существует угроза нарушения их прав, предусмотренных законодательством. Одной из важных мер будет являться виктимологическая профилактика, в том числе, соблюдение определенных правил безопасности при использовании сети «Интеренет». Сформулированные нами правила безопасного поведения в сети обезопасит несовершеннолетних от противоправных посягательств при нахождении в интеренет-пространстве в рамках его использования.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конституция Российской Федерации (принята всероссийским голосованием 12 декабря 1993 г.) [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.
2. Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних: Федеральный закон от 24 июня 1999 г. № 120-ФЗ // [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.
3. О защите детей от информации, причиняющей вред их здоровью и развитию: Федеральный закон от 29 декабря 2010 г. № 436-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.
4. Об информации, информационных технологиях и защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.
5. О противодействии терроризму: Федеральный закон от 6 марта 2006 г. № 35-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.
6. О противодействии экстремистской деятельности: Федеральный закон от 25 июня 2002 г. № 114-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.
7. Концепция информационной безопасности детей: распоряжение Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.
8. Об утверждении Концепции развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2025 года: распоряжение Правительства Российской Федерации от 22 марта 2017 г. № 520-р // [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.
9. Об утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года: распоряжение Правительства Российской Федерации от

29 мая 2015 г. № 996-р [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.

10. 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: постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.

11. Об утверждении Инструкции по организации деятельности подразделений по делам несовершеннолетних органов внутренних дел Российской Федерации: приказ МВД России от 15 октября 2013 г. № 845 [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.

12. Об утверждении Критериев оценки материалов и (или) информации, необходимых для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерством внутренних дел Российской Федерации, Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека, федеральной налоговой службой о включении доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие запрещенную информацию, в единую автоматизированную информационную систему Единый реестр доменных имен, указателей страниц: приказ Роскомнадзора № 84, МВД России № 292, Роспотребнадзора № 351, ФНС России ММВ-7-2/461@ от 18 мая 2017 г. [Электронный ресурс] // СПС «КонсультантПлюс». – URL: https://www.consultant.ru.

13. *Акаева К. А.* К вопросу о противоправной деятельности «групп смерти» / К. А. Акаева, Ю. А. Западнова // Эпомен. – 2020. – № 41. – С. 213–223.

14. *Антонян Ю. М.* Психология преступника и расследования преступлений / Ю. М. Антонян, М. И. Еникеев, В. Е. Эминов. – Москва, 1996. – 336 с.

15. Расширенное заседание коллегии МВД России [Электронный ресурс] // Официальный сайт Президента Российской Федерации. – URL: http://www.kremlin.ru.

16. *Ермолин А. В.* Юридико-психологические аспекты вовлечения молодежи в деструктивные интернет-сообщества / А. В. Ермолин, И. Г. Чапайкина // Вестник Костромского государственного университета. – 2017. – № 4. – С. 89–93.

17. *Иванов Р. А.* Выявление лиц, подверженных влиянию деструктивной молодежной субкультуры «Колумбайн» и склонных к экстремистким действиям: метод. рекомендации / Р. А. Иванов, М. В. Швецов, В. Н. Германович. – Минск: Ин-т нац. безопасности Республики Беларусь, 2019. – 36 с.

18. Методическое пособие по выявлению признаков риска поведения в социальных медиа [Электронный ресурс] // Официальный сайт АО «Крибрум». – URL: https://www.kribrum.ru.

19. Официальный сайт Объединенной редакции МВД России. – URL: http://www.ormvd.ru.

20. Официальный сайт Всемирной организации здравоохранения. – URL: https://www.who.int.

21. Поведенческие маркеры учащихся группы риска [Электронный ресурс] // Официальный сайт Челябинского института развития профессионального образования. – URL: http://chirpo.ru.

22. *Щетинина Е. В.* Социальные сети Интернета: популяризация «культуры смерти» в подростковой среде [Электронный ресурс] / Е. В. Щетинина // HomoCyberus. – 2018. – № 2 (5). – URL: http://journal.homocyberus.ru.

23. *Щетинина Е. В.* Проблемы развития культуры насилия в интернет-пространстве / Е. В. Щетинина // Инновационное развитие профессионального образования. – 2018. – № 2 (18). – С. 127–130.

Приложение А

Правила безопасного поведения несовершеннолетних в виртуальной среде

Компьютерные вирусы.

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (копированию). В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через Интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ.

2. Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его.

3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере.

4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз.

5. Ограничь физический доступ к компьютеру для посторонних лиц.

6. Используй внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников.

7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI.

С помощью WI-Fi можно получить бесплатный интернет-доступ в общественных местах: кафе, отелях, торговых центрах и аэропортах. Также является отличной возможностью выхода в Интернет. Но многие эксперты считают, что общедоступные Wi-Fi-сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-Fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi-сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера.

2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое устройство.

3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе.

4. Не используй публичный Wi-Fi для передачи личных данных, например, для выхода в социальные сети или в электронную почту.

5. Используй только защищенное соединение через HTTPS, а не HTTP, т. е. при наборе веб-адреса вводи именно «https://».

6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети.

Социальная сеть – это сайт, который предоставляет возможность людям осуществлять общение между собой в Интернете. Чаще всего в них для каждого человека выделяется своя личная страничка, на которой он указывает о себе различную информацию, начиная от имени, фамилии и заканчивая личными фотографиями. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе необязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей.

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы.

3. Защищай свою репутацию – держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить.

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: место жительства, место учебы и прочее.

5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение.

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Мошенничество с использованием электронных средств платежа (электронные деньги).

Электронные деньги – это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги. Электронные деньги появились совсем недавно, и именно из-за этого во многих государствах до

сих пор это явление не получило своего отражения в законах. В России же они функционируют и законодательно урегулировано, закон их разделяет на несколько видов – анонимные и не анонимные. Разница в том, что анонимные – это те, с которыми разрешается проводить операции без идентификации пользователя, а идентификация пользователя для не анонимных является обязательной. Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства.

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля.

3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли – это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т. п. Например, StROng!;;

4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта.

Электронная почта – это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также, кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В Интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге.

2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13».

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS.

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность.

6. Используй несколько почтовых ящиков. Первый – для частной переписки с адресатами, которым ты доверяешь. Этот электронный адрес не надо использовать при регистрации на форумах и сайтах.

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Кибербуллинг или виртуальное издевательство («троллинг»).

Кибербуллинг – преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт.

2. Управляй своей киберрепутацией.

3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.

4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.

5. Веди себя вежливо.

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.

7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.

8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон.

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

1. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.

2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

3. Необходимо обновлять операционную систему твоего смартфона.

4. Используй антивирусные программы для мобильных телефонов.

5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.

6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.

7. Периодически проверяй, какие платные услуги активированы на твоем номере.

8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.

9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Незаконное распространение, в том числе хищение личных данных.

Главная цель фишинг – вида интернет-мошенничества – состоит в получении конфиденциальных данных пользователей – логинов и паролей. На английском языке phishing читается как фишинг (от fishing – рыбная ловля, password – пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее.

2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем.

3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем.

4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты.

5. Установи надежный пароль (PIN) на мобильный телефон.

6. Отключи сохранение пароля в браузере.

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Приложение Б

Правила безопасного интернет-знакомства

1. Обращай внимание на содержание аккаунта своего нового друга. Указывает ли он свое настоящее имя и фамилию? Есть ли у него реальные друзья? Насколько долгая история создания его аккаунта? Есть ли личные фотографии? Указана ли личная информация – школа, университет, город? В каких сообществах состоит человек?

Должно насторожить: отсутствие реального имени (никнейм), а также упоминаний личной информации и реальных фотографий; непродолжительная история аккаунта; наличие фейковых друзей; подписки на сообщества, содержащие деструктивный контент.

2. Обращай внимание на вопросы, которые задает тебе новый друг – спрашивает ли он личную информацию – домашний адрес, график и место работы родителей, доход семьи? Не уходит ли от ответов на вопросы о своей жизни?

Должно насторожить: нежелание собеседника рассказывать о своей личной жизни, прямые или косвенные вопросы про твою интимную жизнь, финансовое благополучие, подробные вопросы об отношениях с родителями.

3. Не задает ли собеседник слишком личные вопросы? Не просит ли выслать твои интимные фотографии? Приглашает ли тебя встретиться у себя дома или в малолюдном месте?

Должно насторожить: просьба прислать свои интимные фотографии или получение интимных фотографий собеседника; вопросы, связанные с твоей интимной жизнью; приглашение со стороны незнакомого собеседника встретится с тобой у него дома, в гостях или в малолюдных и незнакомых для местах, а также попытки собеседника прийти к тебе в гости.

4. Не заводит ли собеседник частые беседы о религии или политике? Не пытается ли он навязать тебе свою позицию как единственно верную?

Должно насторожить: агрессивные попытки собеседника навязать свою точку зрения, требование полного подчинения его авторитету, использование манипулятивных техник.

5. Не заявляет ли собеседник свою позицию как попытку тебе помочь, утверждая, что никто, кроме него, не сможет понять тебя?

Должно насторожить: активная критика со стороны собеседника твоих друзей и близких (попытки обвинить круг общения в твоих проблемах), а также твоих убеждений или образа жизни.

6. Не предлагает ли он тебе получить материальных доход – быстрый, легкий, высоко оплачиваемый?

Должно насторожить: предложения со стороны собеседника повысить твой доход за счет лишь предоставления номера твоей кредитной карты или карты твоих родителей; просьба передать посылку незнакомым людям за

хорошее вознаграждение, а также просьбы перевода денежных средств в качестве срочной помощи в трудностях собеседника.

Если ты столкнулся с опасным собеседником, следует:

1) немедленно прекратить общение;

2) сообщить о данном факте взрослым (родителям/педагогам);

3) при столкновении с реальными случаями склонения к интимному разговору, вступлению в радикальные организации и др. необходимо сделать скрин переписки (не удаляйте переписку до завершения оперативных действий!) и отправить его на горячую линию «Скажи экстремизму – НЕТ» (http://resurs-center.ru/hotline) или в аккаунт в социальной сети «Вконтакте» – «ЭКСТРЕМИЗМУ НЕТ» (https://vk.com/nes74).

Будьте внимательны!

Берегите себя и своих близких!

Контакты для получения региональной методической и ресурсной помощи:

– Виртуальная горячая линия «Кибербезопасность»:
http://www.resurs-center.ru/hotline

– Онлайн-консультант по вопросам медиабезопасности:
http://www.resurs-center.ru

– Бесплатные онлайн-консультации психолога:
https://resurs-center.ru/pomogite-mne

– Всероссийский телефон доверия – 8 800 2000 122.

Содержание

Организация профилактической работы в сфере противодействия вовлечению детей и подростков в деструктивные интернет-сообщества

Учебно-практическое пособие

Редактура и компьютерная верстка *И. Б. Бебих*

Подписано в печать 30.11.2021. Формат 60х84 1/16
Печать трафаретная. Бумага офисная
Усл. печ. л. 2,0. Уч.-изд. л. 2,5
Тираж 86 экз. Заказ № 80

Типография научно-исследовательского
и редакционно-издательского отдела
Уральского юридического института МВД России

620057, Екатеринбург, ул. Корепина, 66