ЦИФРОВЫЕ УГРОЗЫ ДЕТСКОЙ БЕЗОПАСНОСТИ

Краткое пособие для организации
просветительской деятельности

РОЦИТ

НЕ ДОПУСТИ!

International Centre
FOR MISSING & EXPLOITED CHILDREN

СОДЕРЖАНИЕ

Уважаемые коллеги!

В последние годы тема контентной безопасности несовершеннолетних приобрела исключительную актуальность, в связи с чем предпринимаются активные шаги по организации информационно-просветительской деятельности, повышающей осведомленность относительно контентных Интернет-опасностей и способствующей профилактике как Интернет-угроз, так и девиантного поведения несовершеннолетних и искажения их социализации. Для этих целей используются возможности средних образовательных учреждений, тематических кружков для детей и подростков, культурных учреждений, а также Интернета, причем в некоторых случаях такой деятельности пытаются придать системный характер. Тем не менее, при уже сформировавшемся понимании необходимости подобных мероприятий, желающие их организовать специалисты испытывают недостаток информации, которая может быть преподнесена слушателям на этих мероприятиях, а зачастую даже недостаток четкого представления, о чем конкретно должна идти на них речь. Нередко случается и так, что начинающий специалист «тонет» в объеме информации, в том числе вполне доступно изложенной, но всеобъемлющей – в то время как на своей стадии он нуждается в получении базовых «установочных» представлений о предмете.

Наша брошюра предназначена именно для тех случаев, когда специалисту, желающему заниматься информационно-просветительской работой в сфере контентной цифровой безопасности детей и подростков, необходимо

получить базовое представление о проблеме и ее характеристиках – в том числе для того, чтобы определиться с дальнейшим подбором специализированных материалов и литературы. В брошюре охватываются основные контентные угрозы в Интернете для несовершеннолетних, даются их краткие характеристики, специфика опасности и базовые действия по прекращению оборота этих видов контента. Создатели брошюры подразумевают, что, исходя из кратких описаний Интернет-угроз, ее читатели смогут не только определиться с путями расширения своего кругозора, но и получить базовые навыки по профилактике таких угроз.

С уважением,

Центр безопасного Интернета –

«НеДопусти!»

ВОВЛЕЧЕНИЕ НЕСОВЕРШЕННОЛЕТНИХ В СЕКСУАЛЬНУЮ ЭКСПЛУАТАЦИЮ

Несмотря на то, что угроза возникла в незапамятные времена (дела про растление малолетних рассматривались еще в древнеримских судах), с глубоким проникновением в общество сначала фотографии, а затем и цифровых технологий, данный вид угроз для несовершеннолетних получил «новую жизнь». Сущность угрозы заключается в производстве, распространении и сбыте материалов со сценами сексуальной эксплуатации несовершеннолетних, то есть сексуальных действий с участием хотя бы одного несовершеннолетнего либо обнажения несовершеннолетнего. Такие материалы распространяются в форме фото, видео, текстовых описаний, рисованных картинок.

Традиционно распространение сцен сексуальной эксплуатации несовершеннолетних рассматривается как самостоятельная угроза, хотя специалисты – сначала осторожно, затем более отчетливо – относят ее к числу угроз против чести, достоинства и репутации жертвы. Ключевая опасность данной угрозы именно в факте распространения информации, которая негативно воздействует на честь, достоинство, репутацию и внешнее восприятие жертвы.

Более того, в Интернете любая информация может «всплыть» даже спустя годы после того, как она была создана и удалена, нанося таким образом урон психике и репутации бывшей жертвы (в том числе прошедшей психологическую реабилитацию).

Последствия этого могут затрагивать семейную и рабочую жизнь бывшей жертвы, провоцировать неврозы и даже самоубийства.

Как правило, подобный контент выявляется лишь применительно к одному месту расположения (хостингу). Несмотря на появление программно-технических механизмов, способных находить копии выявленных изображений по всему Интернету (и, соответственно, содействовать их удалению), полной гарантии того, что данная информация не «проявится» вновь спустя годы, дать никто не может. Все это усиливает опасность, исходящую от подобного контента и от факта его распространения, превращая по сути преступление в длящееся.

Второй опасный аспект такого контента – эксплуатация интереса к сексу с несовершеннолетними. Среди отдельных групп специалистов существует устойчивая точка зрения, что регулярное потребление подобного контента может спровоцировать потенциального злоумышленника на реальное преступление против половой неприкосновенности несовершеннолетнего. Тем не менее в настоящее время при борьбе с распространением сцен сексуальной эксплуатации несовершеннолетних доминирует подход, исходящий из концепции защиты прав и законных интересов реальных жертв – борьба с возможной эксплуатацией интереса к сексу с несовершеннолетними, несмотря на осуждение самого явления, вызывает у специалистов и законодателей многих стран сомнения ввиду своей нечеткости и создания опасного прецедента.

Исходя из «идеологического обоснования» вредоносности и борьбы с контентом, ключевое значение имеет определение жертвы противоправного контента. Если брать Россию, то, согласно российскому законодательству, жертва подобного преступления – это реальный несовершеннолетний. Закон фактически требует достоверную идентификацию жертвы как реального несовершеннолетнего, в связи с чем в настоящее время в России к детской порнографии относятся лишь фотовидеоизображения с сексуальной эксплуатацией реальных детей. В результате эксплуатация интереса к сексу с несовершеннолетними фактически остается слабонаказуемой – к именно детской порнографии не относятся текстовые описания секса с детьми, а также недокументальные (художественные) изображения персонажей с чертами несовершеннолетних (работы художников, аниме\хентай

и т.п.). Также в настоящее время нельзя по российскому закону отнести к детской порнографии изображения, где совершеннолетним персонажам придан имидж несовершеннолетних (например, старшеклассников). Следует отметить, что в отношении почти всего вышеперечисленного со стороны отдельных законодателей предпринимаются устойчивые попытки криминализовать подобный контент именно как «детскую порнографию», и соответствующий законопроект проходит рассмотрение в российской Государственной Думе – в частности, предлагается внести в соответствующую статью российского уголовного закона текстовые описания сексуальных действий с несовершеннолетними и эксплуатации совершеннолетними персонажами имиджа несовершеннолетних. До принятия законопроекта (хотя это «размоет» идеологическую концепцию криминализации контента) определенная борьба с подобным контентом возможна в рамках законодательства, криминализующего распространение порнографии вообще (а не специфически детской).

По международной статистике, основная часть жертв приходится на предподростковый и подростковый возраст (до так называемого «возраста согласия», когда лицо получает право законно вступать в половые отношения).

Преимущественно жертвами являются лица женского пола, хотя весьма высок процент и жертв мужского пола (81% девочек против 13% мальчиков по данным INHOPE за 2014 год).

Изготовление сцен сексуальной эксплуатации несовершеннолетних нельзя назвать «обособленным» преступлением, так как оно прямо вытекает из другого преступного деяния - собственно факта сексуальной эксплуатации несовершеннолетних (хотя, с точки зрения следствия, оператор может сам не совершать сексуальных действий с детьми). **Сексуальная эксплуатация вовсе не означает обязательного полового акта взрослого с ребенком – достаточно вовлечения детей в совершение некоторых действий, понимаемых законом как сексуальные (развратные), в том числе «бесконтактно» (через Интернет).** Закон, как правило, содержит четкие критерии отнесения изображений к сценам сексуальной эксплуатации, при этом в законодательствах разных стран могут присутствовать определенные отличия. К примеру, фотографии «детей-моделей» без обнажения половых органов российский закон к детской порнографии не отно-

сит, в то время как в некоторых центральноевропейских странах такой контент будет рассматриваться так же, как половой акт с ребенком.

Вопреки распространенному стереотипу, похищения детей специально для съемок детской порнографии происходят крайне редко. Двумя основными способами вовлечения несовершеннолетних в создание подобного контента являются злоупотребление доверием детей (обман), последствием которого может стать шантаж, и самостоятельное предложение несовершеннолетними сексуальных действий и услуг (различные формы «детской проституции»). В качестве основной «группы риска» выделяются дети, оказавшиеся в трудной жизненной ситуации и вынужденные полагаться на себя (дети, убежавшие из дома, занимающиеся бродяжничеством, воспитанники детских домов, дети, вовлеченные в попрошайничество). «Вербовщиками» могут выступать не только взрослые, но и другие несовершеннолетние. В качестве мотиватора выступают либо вознаграждение (денежное, иное материальное, совершение неких действий в пользу несовершеннолетнего) либо уже упомянутый шантаж (угроза распространения порочащей информации, реже – насильственных действий).

Нередко несовершеннолетние (в подавляющем большинстве случаев подростки) самостоятельно выкладывают свои сексуализированные изображения в Интернете, как правило, в поисках дополнительной популярности (так называемый «секстинг»).

Зачастую подобные изображения выкладываются в Интернет через мобильные устройства – на которые обычно и делаются такие фото или видео. Секстинг обычно рассматривают как один из факторов, благодаря которым к жертве привлекается внимание лиц, имеющих умысел на сексуальную эксплуатацию несовершеннолетних, однако он и сам по себе является самостоятельной Интернет-угрозой репутационного характера. Принадлежность к «группе риска» в случаях секстинга необязательна – мировая практика показывает, что на публикацию подобных изображений идут подростки с вполне благополучной социальной обстановкой, а причиной этого является «поиск популярности».

Интернет, по мере его развития, стал весьма активно использоваться для распространения и публичной демонстрации изображений противоправной эксплуатации несовершеннолетних (причем в глобальном масштабе, чего ранее не было) – и, более того, поиск и выбор жертв в последние годы нередко осуществляется именно в Интернете. Всемирная Сеть является удобной коммуникационной площадкой, обеспечивающей контакт с интересующим персонажем за тысячи километров, и при этом обеспечивающей относительную анонимность (в том числе через создание «ложной идентичности» - когда злоумышленник намеренно выдает себя за другое лицо, к примеру, сверстника). **В настоящее время основным местом выхода злоумышленника на контакт являются социальные сети, однако такой контакт возможен и на других коммуникационных площадках (в чатах, форумах, гораздо реже в Twitter, а также в сервисах типа Instagram).** В большинстве случаев злоумышлен-

ники – хорошие психологи, поэтому им удается установить необходимый уровень контакта с жертвой и завоевать ее доверие. К примеру, собеседник может оказать помощь и поддержку в проблемах жертвы с родителями и сверстниками. В ходе общения оно может начать приобретать сексуализированный характер (обсуждение интимных тем, сексуальных действий и поведения, обмен мнениями и даже изображениями), однако в некоторых случаях этого может и не происходить – если злоумышленник делает ключевую ставку на «реальную встречу».

«Реальная встреча», то есть назначение встречи вне Интернета, является наиболее опасным элементом вовлечения, потому что, как правило, именно там следует предложение вступить в сексуальные отношения.

Такое предложение может поступить как на первой встрече, так и на последующих – в зависимости от стратегии вовлечения, выбранной злоумышленником, в частности от той идентичности, которой он пользовался на стадии вовлечения в Интернете. В некоторых случаях вовлечение производится без назначения «реальной встречи» - путем склонения к совершению сексуальных действий перед веб-камерой или отправке собственных «эротических» фотовидеоизображений. На определенной стадии такое склонение приобретает форму шантажа – как правило, в тот момент, когда жертва отказывается продолжать дистанционный контакт в сексуальном ключе. На практике шантаж сводится к угрозам разослать ранее полученные сексуальные изображения жертвы по

кругу знакомых, родителям, а также выложить их в общий публичный доступ. Целью такого шантажа может являться как продолжение дистанционного сексуального контакта (в том числе ради получения новых изображений), так и назначение реальной встречи для перевода сексуальной эксплуатации жертвы в оффлайновую стадию. Следует отметить, что данный прием характерен не только для несовершеннолетних жертв, но и для потерпевших старше 18 лет.

Интернет благодаря своей распространенности, трансграничности и относительной анонимности играет большую роль в распространении изображений со сценами сексуальной эксплуатации детей. Он используется злоумышленниками как бесконтактный, трансграничный и относительно анонимный способ передачи подобной информации – как в закрытых сообще-

ствах, так и в публичный доступ. Так же, как и в случае с вовлечением детей, для распространения нередко используются социальные сети (особенно при распространении на неопределенный круг лиц), которые в последнее время начинают вытеснять специализированные сайты. Помимо социальных сетей, для закрытого или относительно закрытого распространения сцен сексуальной эксплуатации несовершеннолетних активно используются торрент-сети, являющиеся средством адресной доставки подобного контента. Закрытые сообщества также создаются в форме форумов или блогов.

В связи с тем, что в сексуальную эксплуатацию нередко вовлекаются несовершеннолетние из «групп риска», проблема сексуальной эксплуатации детей весьма тесно переплетается с проблемой детей, покинувших свое место пребывания. Работа по предупреждению сексуальной эксплуатации детей оказывает позитивный эффект на соответствующие «группы риска», предупреждая их вовлечение в данный вид социальной угрозы. Практическая работа по выявлению фактов сексуальной эксплуатации помогает в выявлении пропавших или похищенных детей, а также помогает грамотной организации реабилитационной работы, которая ведется из расчета терапии двух угроз личности ребенка. Именно в связи с этим в последнее время наметилась тенденция по сращиванию проектов по оказанию помощи пропавшим детям и эксплуатируемым детям, в том числе на базе «Горячих линий» по противоправному контенту. Такое сращивание подразумевает перекрестную проверку информации по базам данных о противоправной эксплуатации и о пропавших детях, комбинированную

информационно-просветительскую работу, комплексные консультативно-реабилитационные действия, расширенный спектр аналитических мероприятий по полученным «Горячими линиями» сигналам.

В зависимости от целевой аудитории, пользователям предлагаются как государственные, так и общественные механизмы выявления и прекращения оборота подобного контента, а также технические средства самозащиты от нежелательного доступа к нему несовершеннолетних.

«Личные» программно-технические средства принято обозначать не совсем точным общим названием «Родительский контроль». Речь идет о специализированных программах, функциях в другом программном обеспечении и о специализированных тарифах, посредством которых осуществляется фильтрация запрашиваемого пользователем контента. Правовой базой для таких средств в России является в первую очередь Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию», а также ч.6 ст.10 Федерального закона «Об информации, информационных технологиях и защите информации». Большинство современных средств «родительского контроля» построены по принципу так называемых «белых списков», разрешая доступ к изначально проанализированному контенту, теоретически исключающему доступ к контенту, опасному для психики, мировоззрения и физической неприкосновенности детей. Подобные программно-тех-

нические решения могут предлагаться как отдельным продуктом, так и в качестве отдельной функции защитного программного обеспечения с широким функционалом (например, «Лаборатория Касперского»), а также могут присутствовать непосредственно в операционной системе (Windows 7,8, 10). **Функции специализированного доступа к «детскому Интернету» предлагаются также социально-ответственными Интернет-провайдерами (так называемые «детские тарифы», к которым необходимо специально подключиться).** Как правило, такие фильтры защищены от несанкционированного отключения детьми, при этом не стесняют взрослых при необходимости поиска информации за пределами «белого списка». Однако следует учитывать, что ни один «контентный фильтр» не гарантирует стопроцентной защиты от противоправного контента; при этом отдельные решения могут предотвращать доступ детей и подростков к популярным среди них Интернет-ресурсам, которые тем не менее были сочтены небезопасными создателями защитных программно-технических решений (например, может ограничиваться доступ к социальной сети «ВКонтакте»). Также необходимо знать, что подобные решения в большинстве случаев рассчитаны на «стационарные» компьютеры и ноутбуки и, как правило, не охватывают мобильные устройства (смартфоны и планшеты под управлением ОС для мобильных устройств) – защитные программы для мобильных устройств в настоящее время, по сути, единичны. Тем не менее производители все шире и шире начинают предлагать мобильные средства ограничения доступа к нежелательному для детей контенту, в связи с чем – а также с ростом популярности мобильного Ин-

тернета у несовершеннолетних – крайне целесообразно установить подобное решение на смартфон или планшет, которым пользуется ребенок.

При выявлении контента, потенциально подпадающего под определение детской порнографии, пользователь может принять участие в прекращении оборота такого контента следующими путями:

- Оставить заявление в электронной форме на сайте правоохранительного органа (например, Единый портал правоохранительных органов 112.ru). Минусом подобного решения является обязательная идентификация заявителя (так как анонимные сообщения не могут являться основанием для возбуждения уголовного дела) и потенциальный непосредственный контакт с представителями правоохранительных органов в оффлайне.

- Сообщить о противоправном контенте в Роскомнадзор (rkn.gov.ru). При обращении в данный орган следует учитывать, что:
  - В отличие от общественных «Горячих линий», при отсутствии реакции провайдера или владельца контента на уведомление из Роскомнадзора, данный орган ограничивается блокированием доступа к сообщенному контенту. Однако данная блокировка не затрагивает доступа к контенту из-за пределов России и на практике легко обходится при помощи легальных программно-технических средств (анонимайзеров), то есть данный контент остается доступен даже после реакции уполномоченного органа;
  - Несмотря на техническую возможность подачи анонимного сообщения, публичный регламент данного сервиса просит «в обязательном порядке указывать свои фамилию, имя и отчество» при направлении обращения.

- Обратиться непосредственно к администрации ресурса. Социально-ответственный хостинг- или контент-провайдер наверняка отреагирует на Ваше обращение. Однако необходимо учитывать и высокую вероятность отсутствия какой-либо реакции.

- Обратиться на общественную «Горячую линию» по борьбе с противоправным контентом (в настоящее время в России такая линия действует при Центре «НеДопусти!», ранее также имелась «горячая линия» Фонда «Дружественный рунет»). В данном случае обеспечивается полная анонимность обра-

щения, независимость экспертизы и цель непосредственно прекращения публичного доступа к контенту. Однако следует учитывать, что общественная «Горячая линия» не является правоохранительным органом и не имеет распорядительных полномочий, работая по принципу «общественно-государственного партнерства».


BULLYING
STOP
CYBER BULLYING

КИБЕРУНИЖЕНИЕ

В российской практике в это понятие входят собственно киберунижение (по-английски «кибербуллинг» – то есть травля, унижение достоинства и оскорбления в Интернете) и распространение сцен физического насилия над детьми, так как оно зачастую неотделимо от унижения, и целью распространения такого контента нередко является именно унижение жертвы. Данная угроза, по мнению большинства экспертов, является гораздо более массовой, чем распространение сцен сексуальной эксплуатации детей, и при этом не менее опасной – так как осуществляет посягательство на те же права детей-жертв, что и детская порнография. При этом для киберунижения характерна практически любая форма распространения информации в Интернете (текстовая, аудио, фото, видео, реже - недокументальные изображения).

Киберунижение является главной угрозой, посягающей на честь, достоинство и репутацию жертвы вне зависимости от возраста.

Особую опасность киберунижение представляет для несовершеннолетних ввиду повышенного уровня доверия к информации из Сети, специфики подростковой агрессивности, неосознания в полной мере последствий деяния и последующей ответственности, повышенной психологической виктимности несовершеннолетних. В некоторых случаях физическое насилие может сочетаться с элементами сексуального унижения и полноценной сексуальной эксплуатации. Киберунижение как

Интернет-угроза представляет повышенную опасность ввиду трансграничности Интернета и потенциальной повторной публикации спустя годы (как и в случае с детской порнографией). Следует учитывать, что большинство методов и средств защиты, используемых применительно к борьбе с детской порнографией, в случае с кибернижением неэффективны (к примеру, программно-техническая фильтрация контента, поиск копий унижающего контента по хостинг-площадкам и т.п.). Единственным относительно эффективным средством, помимо профилактики, является максимально оперативное прекращение доступа к контенту с материалом кибернижения, включая как удаление контента, так и минимизацию доступа к нему (например, через поисковики – на что направлен российский «Закон о достоверной информации»).

Кибернижение крайне негативно воздействует на самооценку и социализацию детей. Ситуация усугубляется тем, что рекомендуемые в случаях оффлайновой травли ребенка методы изменения «ближнего круга» (перевод в другую школу, переезд в другой район\город и т.п.) в случае с Интернет-кибернижением не работают ввиду трансграничности Интернета – не исключено, что информация о факте насилия или унижения окажется доступной через Интернет и в новом окружении ребенка. В результате, кибернижение способно провоцировать не только неврозы и другие заболевания неврологического или психиатрического характера, но и прямо стимулировать детские суициды (в России с 2013 года такая связь считается доказанной). Кибернижение способно провоцировать ребенка так-

же на самостоятельную смену своего окружения в форме побегов\уходов из дома. Негативное влияние на характер ребенка может выразиться в развитии желания мести, которое в некоторых случаях (например, травли по национальному признаку, внешности и т.п.) может результироваться в увлечение ребенком преступными или экстремистскими группами, прямо стимулировать вовлечение ребенка в такие группы из желания отомстить социальной группе, с которой ребенок ассоциирует своих обидчиков.

Жертвой классического киберунижения может стать любой несовершеннолетний, активно коммуницирующий в онлайн-пространстве.

Для киберунижения характерна плотная связь между онлайн- и оффлайн-действиями, то есть некие действия в оффлайне могут служить стимулом для киберунижения - равно как и онлайн-коммуникация, в свою очередь, может спровоцировать оффлайн-травлю (в том числе с последующей публикацией в сети Интернет). Фактором риска для несовершеннолетних является стремление к самоутверждению, которое зачастую препятствует следованию профилактическим советам по купированию киберунижения (к примеру, подросток далеко не всегда последует совету выйти из дискуссии, где имеет место его унижение). Следует учитывать, что сцены киберунижения, как правило, распространяются в социальных сетях с недостаточным уровнем модерации, а также на популярных среди несовершеннолетних фотовидеохостингах, при этом ссылки на процесс (если он длящийся)

или на информацию о киберунижении могут распространяться среди целевой аудитории (например, знакомых жертвы киберунижения).

Как уже говорилось, основная опасность, добавляемая в процесс унижения ребенка благодаря Интернету – это массовое распространение унижающей честь, достоинство и репутацию ребенка информации, причем данная информация может распространяться как на определенный круг лиц (например, на тех, кто знают жертву лично), так и на неопределенный круг лиц (к примеру, находиться в публичном доступе в социальной сети). Традиционные методы, сопутствующие реабилитации жертвы (смена социального окружения), в условиях трансграничности Интернета могут не работать, так как сохраняется риск доступа нового социального окружения к информации с киберунижением. В подавляющем большинстве случаев агрессорами выступают также несовершеннолетние (либо молодежь), однако можно столкнуться и со случаями, когда несовершеннолетний подвергается унижению и со стороны взрослого\взрослых (видеосъемки унижения учащегося со стороны учителя, реже – «кампания» по направленному унижению заведомого подростка на коммуникационных ресурсах со стороны более старших пользователей). Ввиду прочно укоренившегося мифа о большей безопасности от прямых санкций в Интернет-пространстве, Интернет-сервисы рассматриваются агрессорами как наиболее предпочтительное место для агрессии в отношении окружающих, причем это особенно характерно для пользователей подросткового и молодежного возраста. Опасность киберунижения также усугубляется

тем, что для некоторых категорий детей (со слабой оффлайн-социализацией) Интернет-коммуникационные сервисы являются предпочитаемым коммуникационным каналом, который не может быть адекватно замещен оффлайн-альтернативой.

Случаи похищения детей исключительно для производства контента со сценами физической эксплуатации на практике единичны.

С учетом специфики киберунижения как угрозы, роль профилактики как ключевого элемента предотвращения киберунижения значительно выше, чем в случае с рядом других угроз.

В частности, к профилактике киберунижения можно отнести выстраивание и поддержание «пространства доверия» между ребенком и взрослыми, стимулирование разнообразия кругов общения ребенка (в таком случае ему будет легче безболезненно расстаться с одной из онлайн-площадок в случае киберунижения на ней), и в первую очередь формирования твердого этического комплекса у ребенка применительно к общению в онлайне и оффлайне. Поддержание «защищенного пространства» в школе или детском клубе\кружке по интересам, при отсутствии адекватных усилий со стороны преподавательского состава, может быть инициировано непосредственно родителями (к примеру, на родительском собрании) – при этом в «защищенное пространство» могут входить эффективное воздействие на детей-агрессоров, «уроки этики» (например, в ходе «классных часов»), наличие эффективного и доверяемого школьного психолога.

Информационную помощь могут оказать тематические информационно-просветительские материалы, содержащие подробные советы по профилактике киберунижения.

Что касается прекращения оборота контента с признаками киберунижения, то в настоящее время могут быть рекомендованы три канала для воздействия на оборот подобного контента:

- Обращение на «Горячую линию» по борьбе с противоправным контентом, действующую в рамках общественно-государственного партнерства. Помимо анонимности обращения, преимуществом этого ка-

нала является возможность использовать практически те же механизмы, что для прекращения оборота сцен сексуальной эксплуатации несовершеннолетних. При этом необходимо учитывать то, что возможности данного сервиса ограничены функционалом общественно-государственного партнерства, то есть необходимо понимать, что такая «Горячая линия» не является правоохранительным органом и потому не имеет тех полномочий, которые предоставлены исключительно правоохранителям. В настоящее время сообщения по контенту, связанному с киберунижением, в России принимаются только проектом «НеДопусти!» в рамках Центра безопасного Интернета (РОЦИТ).

- Обращение к администрации сервиса. Прямой канал коммуникации с площадкой, на которой осуществляется киберунижение. Однако в ряде случаев (к примеру, так называемая «абьюзоустойчивость» сервиса) сервис может отказать в удалении контента ввиду специфики атмосферы общения на нем, либо вообще не отреагировать на обращение.
- Обращение в правоохранительные органы. На практике результативно лишь в некоторых, наиболее вопиющих случаях киберунижения, содержащих признаки нанесения телесных повреждений. С учетом того, что в общественном сознании за пределы понятия «правоохранительные органы» зачастую выносится прокуратура, целесообразно заострить внимание целевых аудиторий на возможности обращения в данный орган, так как он уполномочен рассматривать сообщения о любых потенциальных нарушениях законности. При этом следует учесть,

что рассмотрение обращения в прокуратуру может занимать до 30 дней и при этом исключает анонимность.

Для жертв репутационных угроз, к которым относятся различные формы киберунижения, исключительно важна своевременная и качественная реабилитация. Поскольку киберунижение – это процесс, глубоко травмирующий психику жертвы, весьма ценным представляется повышение осведомленности (как детей, так и родителей) о местах получения качественной профессиональной реабилитационной помощи в онлайне и оффлайне. В частности, ребенок должен быть осведомлен о контактах психологических служб, осуществляющих консультирование несовершеннолетних по телефону и в Интернете (например, Общероссийский детский телефон доверия – 8-800-2000-122), причем Интернет-канал является предпочтительным ввиду большего удобства и доверия к нему со стороны детей. С учетом того, что подобные сервисы предоставляют одноразовое дистантное консультирование (сравнимое со «Скорой помощью»), целесообразно обращение в оффлайне к доверяемому психологу, который сможет в спокойной обстановке провести грамотную реабилитационную терапию. Родителям ребенка-жертвы важно понимать, что «психолог» - не значит «психиатр», обращение к специалисту не является признанием наличия психических отклонений у ребенка и не влечет для него никаких негативных последствий (к примеру, постановки на дискриминационный диспансерный учет в психиатрическом диспансере\кабинете). Непрофессиональная помощь (например, через общение с незнакомцами в Интернете) не только

рискованна в части правильной реабилитации ребенка, но и потенциально опасна в плане вовлечения ребенка в другие Интернет-угрозы, в частности сексуальную эксплуатацию (зарубежная статистика показывает, что дети-жертвы киберунижения являются «группой высокого риска» для потенциальных педофилов, которым состояние ребенка облегчает завоевание доверия и манипуляцию несовершеннолетним).

ВОВЛЕЧЕНИЕ В ПОТРЕБЛЕНИЕ НАРКОТИЧЕСКИХ И ПСИХОТРОПНЫХ СРЕДСТВ

В отличие от двух предыдущих угроз, данную Интернет-угрозу принято относить скорее к «информационным», где Интернет используется как «обходной путь» доставки информации до потенциальных потребителей наркотических, психотропных веществ и их прекурсоров (далее будет использоваться упрощенный термин «наркотики»). Данную угрозу принято делить на две части: пропаганда потребления наркотиков и использование сети Интернет для реализации наркотиков. Зачастую обе этих угрозы взаимосвязаны и могут встречаться на одном и том же Интернет-ресурсе.

Пропаганда и распространение наркотиков – это изначально оффлайновая опасность, перекочевавшая в онлайн ввиду дополнительных возможностей в Интернете (например, доведение информации до максимального количества людей с минимальными затратами) и дополнительной анонимности при осуществлении своей противоправной деятельности, в том числе минимизации оффлайновых контактов с риском задержания правоохранительными органами. Предложение наркотических средств в Интернете распространяется на почти неограниченную аудиторию, которая в оффлайновых условиях злоумышленникам была недоступна. Физическое рас-

положение Интернет-ресурса при этом может быть за пределами российской юрисдикции, что, по ошибочному мнению преступников, повышает их «безопасность». В целях повышения сбыта и притока новых клиентов наркодилеры формируют и поддерживают привлекательный имидж потребления наркотиков, ассоциируют потребление наркотиков с успешностью, весельем и даже медицинской реабилитацией (!). Для повышения доверия к информации используется «псевдонаучный» и «аналитический» антураж, со специфической интерпретацией общедоступных данных либо с вымышленными «открытиями», «достижениями» и т.п. Пользователь также дезинформируется относительно якобы «безвредности» таких средств и препаратов для здоровья, а также относительно легальности их оборота, хранения и употребления. Подобный контент, выполненный на качественном уровне, создает ложное мнение о привлекательности и безвредности потребления наркотиков, способствуя вовлечению в потребление наркотиков несовершеннолетних с повышенным уровнем доверия к информации. При этом пользователю предоставляются возможности бесконтактного приобретения наркотиков онлайн через специфические «магазины» и бесконтактные анонимные формы оплаты, что также понятно и доступно для подростковой и молодежной аудитории.

Для реализации противоправных действий преступники могут использовать различные коммуникационные онлайн-сервисы, главными из которых являются специализированные веб-сайты (обычно на бесплатном

хостинге) и страницы либо сообщества в социальных сетях.

Сбыт наркотиков также может производиться с использованием онлайн-досок объявлений. Реже используются форумы.

В современной практике в основном принято обращать пристальное внимание на чисто оффлайновые последствия угрозы, связанной с пропагандой и распространением наркотиков. Однако существование данной угрозы в онлайне не является каким-то самостоятельным фактором и обусловлено исключительно теми преимуществами, которые злоумышленники могут извлечь из онлайн-коммуникационных технологий – возможностью транслирования заведомо ложной информации под видом достоверной и использованием «ложной идентично-

сти». Также данная Интернет-угроза напрямую связана с Интернет-мошенничеством – нередки случаи, когда сайты и страницы, предлагающие запрещенные вещества, на деле являются ресурсами мошенников, которые исправно собирают с наркозависимых деньги на «вещества», но ничего не присылают взамен. Психологический расчет мошенников очень тонок – обманутый таким образом наркопотребитель стопроцентно не обратится в правоохранительные органы по факту мошенничества, так как это будет равносильно «явке с повинной» в совершении другого преступления, связанного с попыткой приобретения наркотика.

Перенос сбыта наркотиков в Интернет вызван стремлением преступников к максимальной анонимизации и переводу своей «работу» на бесконтактный принцип. Что касается активной пропаганды потребления наркотических средств, то она обусловлена как трансграничностью Интернета (то есть возможностью выбрать максимально «удобную» юрисдикцию), так и большой аудиторией Интернета, в первую очередь среди подростков и молодежи. При этом создание и распространение подобных материалов в Интернете в настоящее время не требует значительных усилий и специальных знаний. Не следует забывать и о повышенном уровне доверия молодых пользователей к «печатному слову», которое идет еще из газетно-книжной эпохи.

Механизмы борьбы с подобным контентом в целом не отличаются от классических механизмов, применяемых в отношении текстово-контентных угроз. Как правило, контентные фильтры, построенные по принципу «бело-

го списка», весьма уверенно предотвращают доступ к подобному контенту – за исключением расположенного в социальных сетях (если доступ к социальным сетям не перекрыт фильтром). Это связано с тем, что для своей деятельности преступники вынуждены использовать специализированные сайты и страницы, которые к тому же регулярно меняют свое расположение, а, к примеру, «доски объявлений» в «белые списки», как правило, не входят. Тем не менее, если такой контент все-таки оказался доступен несовершеннолетним, или родитель

встретил такой контент в свободном доступе, он может предпринять определенные шаги для прекращения его оборота в Сети:

- Обращение непосредственно в правоохранительный орган (после расформирования Федеральной службы по контролю за оборотом наркотиков – ФСКН – таким органом является МВД, то есть полиция). Соответствующие механизмы для онлайн-обращения имеются на сайте МВД. Однако для этого способа характерны все те неудобства, которые были упомянуты в разделе «Борьба с сексуальной эксплуатацией детей» - отсутствие анонимности обращения и потенциальная необходимость тратить личное время на участие в следственных действиях.
- Обращение в Роскомнадзор в соответствии с известным Федеральным законом № 139-ФЗ (о блокировке противоправного контента).

В отличие от первого варианта, здесь теоретически допускается анонимность – однако, как следует из информации профильного портала eais.rkn.gov.ru, предоставление реальных данных заявителя является настоятельной рекомендацией.

Решение о потенциальной противоправности контента в данном случае также выносится профильным правоохранительным органом. Однако, как уже было указано в разделе «Борьба с сексуальной эксплуатацией детей», данный механизм при отрицательном результате уведомления провайдера о необходимости прекращения оборо-

та контента ограничивается лишь его блокированием, в результате чего контент остается доступен при совершении широко известных пользовательских манипуляций.

- Обращение на общественную «Горячую линию» по прекращению оборота противоправного контента. Данный вариант гарантирует анонимность заявителя и при этом ориентирован именно на прекращение публичного оборота противоправного контента. Однако «Горячая линия» не наделена распорядительными функциями – таковые в данном случае осуществляются теми же правоохранительными органами или провайдерами по уведомлению «Горячей линии».

ВОСПИТАНИЕ «КУЛЬТУРЫ НЕНАВИСТИ» У НЕСОВЕРШЕННОЛЕТНИХ, ВОВЛЕЧЕНИЕ ИХ В ПРЕСТУПНЫЕ И ЭКСТРЕМИСТСКИЕ ДЕЙСТВИЯ

Эта информационная угроза стала популярной в последние три десятилетия и прочно «прописалась» в Интернете. Угроза представляет из себя информацию в Интернете, направленную на провокацию ненависти и насилия к людям по признаку их принадлежности к нации, расе или религии, а также пропаганду подобных взглядов и использование сети Интернет для привлечения людей в оффлайновые группировки, осуществляющие насильственные действия в отношении людей определенной национальности, расы или вероисповедания (иногда – также культурной группы). Интернет используется также для вовлечения людей (в первую очередь подростков и молодежи) в обычные преступные группы, в частности хулиганские.

Данная Интернет-угроза представляет опасность в первую очередь для формирующейся системы ценностей несовершеннолетних, прививая им деструктивные ценности, причиняющие вред в последующей социальной жизни. Негативное восприятие лиц

по признаку национальности, расы или религии, как правило, порождает в отношении таких лиц целый ряд угроз, начиная от оскорблений и кончая массовыми насильственными действиями. При пропаганде ненависти, как и в случае с пропагандой наркотиков, может использоваться псевдонаучный, псевдоисторический антураж, фальсификация исторических документов и статистических данных, тенденциозная манипуляция фактами в целях подмены понятий, то есть такая пропаганда мимикрирует под доверяемые образцы информации. Практика показывает, что в некоторых случаях экстремистская идеология граничит с террористической, особенно при наличии соответствующих регионально-культурных предпосылок. При этом данную угрозу следует строго отграничивать от реализации гражданами права на свободу слова и критику органов власти и должностных лиц, которая, согласно решениям ЕСПЧ, может носить также и «шокирующую» форму.

Распространение националистической и расистской информации в Интернете осуществляется практически в любых информационно-коммуникационных сервисах, начиная от специализированных сайтов и заканчивая форумами и социальными сетями.

При ведении пропаганды подобного рода выбираются ресурсы, популярные среди несовершеннолетних,

которые зачастую являются основными целевыми аудиториями злоумышленников. Коммуникационные ресурсы при этом предоставляют возможности присоединения к виртуальным, а затем и реальным группам, осуществляющим те или иные действия по признаку ненависти к той или иной группе. Помимо оффлайновых активностей (насильственных действий, массовых беспорядков), «среда ненависти» может присутствовать и в онлайне – в частности, по сценарию кибермунижения, нанося примерно такой же вред жертве, как и стандартное кибермунижение. Сервисы web 2.0 могут использоваться также для рекрутирования в преступные оффлайновые группы, не связанные напрямую с проявлениями расизма или национализма, но объединяющие участников по возможности группового совершения, к примеру, хулиганских действий, при этом не неся какой-либо структурированной идеологии общественно-политического характера (например, группировки футбольных фанатов – «ультрас»). Как и в случае с пронаркотическим контентом, злоумышленники используют такие свойства Интернета, как огромная аудитория, трансграничность и относительная анонимность, легкость создания и распространения контента для определенной целевой аудитории, возможность удаленной коммуникации в режиме реального времени. Последняя возможность является определяющей для организации и удаленного координирования действий, совершаемых по признаку ненависти – от Интернет-флешмобов до массовых беспорядков.

В последние годы наблюдается значительное «омолодение» жертв данной Интернет-угрозы – подобный контент все чаще направлен на предподростковый возраст, в который происходит формирование социально-этических основ личности. Социальный портрет жертвы довольно расплывчатый, равно как и факторы, стимулирующие к позитивному восприятию подобной пропаганды. Факторами риска могут являться как общее экономическое неблагополучие семьи, так и стремление к социальной справедливости, а также единичные личные инциденты между детьми или подростками разных национальностей (к примеру, одноклассниками) либо детьми и взрослыми. Дополнительный фактор риска – однобокость или ограниченность информационного поля, доступного несовершеннолетнему.

Профилактика и механизмы борьбы с подобным контентом прямо зависят от социальной обстановки, так как популярность экстремальных общественно-политических взглядов свидетельствует о той или иной степени неблагополучия в обществе (зависящего от состояния экономической или политической системы). Тем не менее, наилучшим методом борьбы с подобным информационным воздействием является пополнение информационного поля ребенка или подростка, помогающее ему сформировать социально-неагрессивный взгляд на взаимодействие людей с разными отличительными особенностями и сформировать умение отличать личные характеристики от якобы «общих» черт. Весьма важно, чтобы пополнение информационного поля ребенка осуществлялось не только в оффлайне, но и в Интернете, что обеспечит

должную конкуренцию взглядов на одном канале поступления информации. При этом целесообразно также общее развитие культуры ненасилия, историко-культурного кругозора, предоставление позитивных примеров межнационального и межрелигиозного взаимодействия с маргинализацией радикально-экстремистских взглядов на этнокультурные и социально-религиозные вопросы.

В отличие от ситуации с пронаркотическим контентом, контентные фильтры обеспечивают высокий уровень защиты от данной угрозы только в условиях жесткого «белого списка» и модерации доступных детям коммуникационных ресурсов. При столкновении с контентом, пропагандирующим расовую, национальную или религиозную рознь, призывающим к насилию или массовым беспорядкам по признаку расы, национальности или отношению к религии, а также к иным хулиганским действиям

(включая самоуправные действия по якобы «наведению порядка»), можно предпринять следующие действия:

- Обратиться в прокуратуру. В соответствии с действующим законодательством, прокуратура наделена правом оперативного прекращения оборота подобного контента. При этом следует учитывать, что анонимные обращения прокуратурой не рассматриваются, а также что механизм, доступный органам прокуратуры, является вариантом механизма блокировки доступа к контенту, применяемого Роскомнадзором;
- Обратиться в общественную «Горячую линию» по прекращению оборота противоправного контента. В отличие от прокуратуры, в данном случае основанием для реагирования может стать и анонимное обращение. При этом общественные механизмы, как правило, крайне чувствительны к контенту, который может быть интерпретирован как реализация свободы слова. Однако следует учитывать, что механизмы общественно-государственного партнерства не подменяют государственные органы.

НЕ ДОПУСТИ!

РОЦИТ

СОПРОТИВЛЕНИЕ
правозащитное движение

ОБЩЕСТВЕННАЯ ПАЛАТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Уполномоченный при Президенте Российской Федерации по правам ребенка

INHOPE
ins@fe

International Centre
FOR MISSING & EXPLOITED CHILDREN

KASPERSKY lab