Безопасность детей в сети Интернет.

Концепция информационной безопасности детей утверждена распоряжением Правительства РФ от 2 декабря 2015 года № 2471-р.

Обеспечение информационной безопасности детей возможно исключительно при условии эффективного сочетания государственных и общественных усилий при определяющей роли семьи.

Необходима организация последовательных и регулярных мероприятий государства и общественных организаций, направленных на повышение уровня медиаграмотности детей, которые должны с раннего возраста приобретать навыки безопасного существования в современном информационном пространстве.

Усилия государства по ограничению доступа к ресурсам, содержащим противоправный контент, не смогут полностью оградить детей от вредной информации. Поэтому необходимо формировать у детей механизмы критической оценки получаемых сведений.

Также, необходимо продолжать работу по совершенствованию механизма блокировки сайтов в сети "Интернет", содержащих запрещенную информацию.

Основные опасности в Интернете для детей и подростков следующие:

1. Кибербуллинг (интернет-травля).

2. Использование Интернета для манипуляции сознанием детей и подростков (пропаганда экстремистского, антисоциального поведения, суицидов, вовлечение в опасные игры).

3. "Незнакомый друг" в социальных сетях.

4. Кибермошенничество.

5. Безопасность доступа в Сеть и кража личных данных техническими средствами.

6. Незаконный сбор персональных данных несовершеннолетних и (или) распространение их в открытом доступе.

7. Просмотр сайтов для взрослых.

Куда обращаться в случае интернет – угроз.

Кроме правоохранительных организаций можно обратиться:

1. На горячую линию «Дети онлайн»: 8–800–250–0015 (с 9 до 18 по рабочим дням, звонки по России бесплатные), e-mail:helpline@detionline.com. Это первый в России общественный проект, целями которого является консультирование и оказание психологической помощи детям и подросткам, столкнувшимся со сложностями во время коммуникаций в Интернете.

2. Родители (законные представители) несовершеннолетних могут обратиться в Центр защиты детей от интернет-угроз(ЦЗДИУ) через онлайн - форму. На сайте ЦЗДИУ указано, что Ваше обращение будет рассмотрено в течении 24 часов.

Также сообщается, что Центр работает не только на профилактику, но и на пресечение IT-угроз. Избранное направление деятельности не имеет аналогов, что подтверждается мнением ведущих специалистов и СМИ.

Номер телефона 8 (930) 888-65-15, в будние дни с 09:00 до 18:00 (не указано, что звонок бесплатный - ред.).

3. На Горячую линию Региональной общественной организации «Центр Интернет-технологий» (РОЦИТ). Заполните заявку, приложите нужные ссылки и документы. С вами свяжутся в течение трех дней. Специалисты Горячей линии проконсультируют вас и при необходимости свяжутся с профильными организациями и госорганами, которые могут решить проблему.

4. Подать сообщение в Роскомнадзор о ресурсе, содержащем запрещенную информацию.

5. Оставить свое сообщение о противоправном Интернет-контенте на сайте Лиги безопасного интернета.

1. Кибербуллинг (интернет-травля)

Кибербуллинг

Это травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить кибербуллинг (другое название - троллинг) могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди.

«Троллинг» может принимать разные формы: оскорбления через личные сообщения, публикация и распространение конфиденциальной, провокационной информации о жертве. В интернете, как правило, ребенок находится один на один с потенциальным обидчиком, который к тому же уверен в своей анонимности и может действовать более нагло.

Фейсбук дает следующее определение кибербуллинга: "Травля может происходить где угодно и принимать различные формы — от распространения слухов и размещения нежелательных фото до угроз в чей-то адрес. Под травлей понимается умышленное оскорбление, запугивание и угнетение состояния других людей."

Почти половина российских подростков в 2017 году столкнулась с кибербуллингом, заявил глава Регионального общественного центра интернет-технологий (РОЦИТ) Сергей Гребенников. Об этом сообщает РИА Новости.

Согласно данным, приведенным на международном форуме по кибербезопасности CyberSecurityForum 2018 (CSF 2018), 48% подростков в возрасте 14-17 лет

становились жертвами груминга (шантажа), 46% подростков стали свидетелями агрессивного онлайн-поведения, 44% — получали агрессивные сообщения.

Основные мотивы киберагрессоров это развлечения (46%), власть (40%) и причинение вреда другому и всплеск негатива (35%), отмечается в материалах. При этом, только 17% детей обращаются за помощью к родителям.

Заведующий кафедрой новых медиа и теории коммуникации МГУ им. М.В. Ломоносова Иван Засурский, в мае 2016 года, выразил уверенность, что больше всего на юную психику влияет не тот или иной «взрослый» контент, к которому подросток всегда при желании получит доступ, а кибербуллинг. Явление, о котором в России начали говорить не так давно и опасность которого по-прежнему недооценивается.

«Не надо думать, что существуют какие-то отдельные онлайн-проблемы. Есть подростки, которых никто не воспитывает. Основная угроза для детей — это другие дети. Они бывают очень жестоки», — заявил Засурский.

Психологи и эксперты уверены: важно не следить за каждым шагом ребенка в интернете (зачастую это просто невозможно), а говорить с ним. «Как и в реальном, офлайновом мире, родителям не следует умалчивать о рисках использования интернета, равно как и о его возможностях и безусловной пользе в жизни каждого человека», — считает Денис Жилин из «Разумного интернета».

По мнению эксперта «Лаборатории Касперского», борьба с кибертравлей технически не так проста, поэтому и программный родительский контроль не столь эффективен. При этом дети не способны справиться с агрессорами в одиночку, но зачастую не обращаются за помощью к взрослым, будучи запуганными угрозами, либо просто из-за отсутствия доверия к близким людям. Поэтому самую важную роль в защите ребенка от кибер-террора играют отношения с родителями.

Старший научный сотрудник ESET, Дэвид Харли советует родителям пользоваться интернетом и, в частности, соцсетями вместе со своими детьми, начиная с дошкольного возраста. Это наиболее тактичный способ познакомить их с основами онлайн-безопасности.

2. Использование Интернета для манипуляции сознанием детей и подростков (пропаганда экстремистского, антисоциального поведения, суицидов, вовлечение в опасные игры).

Манипуляция детьми в интернете

Руководитель Центра защиты детей от интернет-угроз Владимир Рогов на вопросы Рамблер, 17.02.2018, в частности, сказал следующее:

- Считаю, что основной интернет-угрозой является манипулятивно-идеологическая вербовка детей в различные движения. Представьте классическую секту, но в соцсетях бывают более изощрённые направления, но смысл тот же — оторвать ребёнка от своего окружения (родители, друзья), приманить к себе, переделать в новый формат.

Также беспокоит напитка молодёжи контентом, который деформирует традиционные российские духовно-нравственные ценности, в частности, антисемейная пропаганда. Это промежуточные звенья цепи, которые доводят детей до «групп смерти» и направления в формате «колумбайн».

С влиянием закрытых групп в социальных сетях связан 1% суицидов несовершеннолетних в России. На первых местах другие причины - неразделенная любовь и конфликты в семье - по 30%. Об этом 30.03.2017 на 5-м Всероссийском форуме "Наши дети" в Петербурге рассказал замначальника главного управления по обеспечению охраны общественного порядка (ГУОООП) МВД России Вадим Гайдов.

Он отметил, что в 2016 году несовершеннолетним в РФ было совершено 720 суицидов, в 2015-м - 685. Об этом сообщает ТАСС.

Вместе с тем в министерстве признали, что в настоящее время особо актуальной становится проблема защиты детей от информации, распространяемой в так называемых закрытых группах, провоцирующих детей на суицид.

Ранее председатель Следственного комитета РФ Александр Бастрыкин сообщил, что сегодня всё большую опасность стали представлять собой "игры на выживание" или "игры на вымирание", организованные в интернете создателями так называемых "групп смерти". "Каждый день сотрудниками Главного управления криминалистики Следственного комитета Российской Федерации выявляются все новые и новые сообщества, которые ставят своей целью уничтожение молодежи", - подчеркнул председатель СК.

3. "Незнакомый друг" в социальных сетях

Исследования показывают, что среди людей, которые заходят на страничку ребенка в соцсетях, каждый второй — это человек, которого он никогда в своей жизни не видел, рассказывает профессор кафедры психологии личности МГУ им. М. В. Ломоносова Галина Солдатова.

"На факультете психологии МГУ мы изучаем новый феномен под названием "незнакомый друг". Это очень большой риск, потому что за каждым из незнакомцев может стоять кто угодно... наши дети... совершенно отчаянно и бесстрашно встречаются с незнакомцами из соцсетей.

Они назначают свидания, ходят по указанным адресам и т. д. Возможно, за дверью их ждет друг на всю жизнь, но с тем же успехом там может оказаться и педофил. Об этом с детьми просто необходимо говорить. Важно, чтобы они ценили приватность своего пространства в интернете точно так же, как ценят приватность своего личного пространства дома...

Ребенок может передать незнакомцам свои персональные данные, поделиться номером кредитки мамы, может сфотографировать квартиру, сообщить адрес, показать интерьер и ценные вещи, рассказать, что семья уезжает в отпуск, и т. д. Нужна очень серьезная кооперация всей

семьи, чтобы уяснить: все, что мы выкладываем в интернет, становится достоянием огромного круга людей, которые далеко не всегда дружелюбно настроены. Мы подготовили специальную книгу для педагогов с уроками для школьников по защите персональных данных. Она может быть полезна и для родителей."

4. Безопасность доступа в Сеть и кража личных данных техническими средствами.

Впервые за все пять лет работы горячей линии «Дети онлайн» на второе место по актуальности вышли вопросы обеспечения безопасного доступа в сеть и защиты от краж личных данных техническими средствами. В 2014 году каждый третий обратившийся сталкивался с блокировкой компьютеров и внедрением на них вредоносных программ и вирусов, а также взломами личных профилей в социальных сетях и блогах.

5. Кибермошеничество

Для кражи личной информации пользователя, применяются все более сложные фишинговые схемы, в том числе с использованием узнаваемых брендов. В 2013 году число обращений по данному вопросу достигло 19%. Чаше всего интернет-пользователи обращались на линию уже после столкновения с мошенниками, чтобы получить консультацию по дальнейшим действиям.

6. Незаконный сбор персональных данных несовершеннолетних и (или) распространение их в открытом доступе

В мае 2014 года Роскомнадзор выявил более 200 сайтов, распространяющих в открытом доступе персональные данные несовершеннолетних россиян и их родителей.

Сайты, разместившие персональную информацию о детях, как правило, принадлежат школам, детским садам, интернатам, а также муниципальным образованиям и администрациям ряда субъектов Российской Федерации.

Обнаруженные данные содержали списки воспитанников детских садов и интернатов, учеников школ, с указанием их ФИО, даты рождения, места проживания, а также сведения о социальном статусе родителей и их принадлежности к той или иной льготной категории граждан. Речь идет о многодетных семьях, матерях-одиночках, безработных родителях, детях сотрудников правоохранительных органов, детях судей, детях, оставшихся без попечения родителей. На сайте одного из образовательных учреждений был опубликован список детей, направляемых на психоневрологическую комиссию.

Как говорится в сообщении Роскомнадзора, "распространение в открытом доступе персональной информации несовершеннолетних может повлечь за собой неблагоприятные последствия для детей и их родителей, связанные с неправомерным посягательством на частную

жизнь семьи, здоровье и половую неприкосновенность детей".

Эксперты очень высоко оценили сайт персональные данные дети, где в занимательной, красочной и очень доступной форме объясняется самое главное из того, что следует знать по этой теме. Лучшей защитой для ребенка будет владение информацией об опасностях, с которыми он может столкнуться в Интернете. Именно в целях информирования о правилах обработки данных был создан этот сайт, - рассказывает зам. руководителя Роскомнадзора Антонина Приезжева.

"Изначально подача сайта была рассчитана на любую целевую аудиторию: от детей до взрослого человека. Замечу, что материалы, тесты, размещенные на портале, можно использовать и в образовательных целях, например, на уроках по интернет-безопасности", - отметила А.Приезжева.

В 2016 году, по сравнению с 2015 годом, было выявлено значительно меньше фактов размещения на официальных сайтах различных учреждений персональных данных детей – прежде число таких случаев выходило за все разумные рамки и объемы.

7. Просмотр сайтов для взрослых

По результатам исследования «Лаборатории Касперского», из всех сайтов с маркировкой 18+ наибольший интерес для российских детей представляют эротические и порнографические сайты - 46,4%, на втором месте оружейная тематика - 26,4%, на третьем - нецензурная лексика - 10,7%.

Следует обратить внимание, что указанные проценты - это удельный вес не всех посещаемых несовершеннолетними сайтов, а только входящих в категорию нежелательных. Ещё точнее - в эти проценты вошли и неудачные попытки попасть на "взрослые" сайты, если они были заблокированы модулем «Родительский контроль».

Сам по себе результат исследования не очень интересен. Чего хочется большинству детей? Поскорее стать взрослыми. И любая маркировка "только для взрослых" еще больше разжигает интерес, считает психолог Елена Кузнецова.

Вывод исследования очевиден - Безопасность ребенка в Сети = Контроль со стороны родителей + «Родительский контроль».

По данным Центра новостей ООН 92% родителей утверждают, что они установили четкие правила поведения для своих детей в Интернете. Однако, эти данные не совпадают с данными опроса детей. 34% детей заявили, что их родители не устанавливали никаких правил и не контролируют то, как они пользуются Всемирной паутиной.

85% родителей сказали, что слышали о программном обеспечении, позволяющем установить родительский контроль на компьютере, которым пользуется ребенок. Но только 30% родителей решили им воспользоваться.

В октябре 2013 года результаты исследования, проведенные Лигой безопасного интернета, МТС и "Лабораторией Касперского" показали, что в России только 21,5% родителей контролируют детей в возрасте от 6 до 17 лет, говоря, на какие сайты заходить можно или нельзя.

Одно из решений этой проблемы - включить опцию "родительский контроль", которая есть у всех антивирусов с InternetSecurity. Кроме этого, можно установить дополнительную программу. Разновидностей этих программ, по доступной всем цене, уже несколько десятков.

Возможно, кого-то заинтересует KinderGate Родительский Контроль. Эту программу от большинства подобных решений отличает следующее:

* невозможно отключить или удалить без знания пароля, заданного при установке;

* корректно работает совместно с любыми антивирусами, поддерживает Linux-системы и Mac OS;

* использует ежедневно обновляемую базу из 500 миллионов сайтов, когда как наборы интернет-ресурсов других решений насчитывают лишь 10-15 миллионов;

* обеспечивает дополнительный уровень защиты посредством инструмента морфологического анализа;

В KinderGate это можно сделать примерно так:

морфологический анализ

* можно контролировать скачивание определенных видов файлов (EXE, DOC, MP3, AVI, и т.д.);

* бесплатный тестовый период 30 дней.

Более подробная информация - на сайте KinderGate Родительский Контроль

Что делать если ребенок смотрит сайты для взрослых?

Например, на вопрос: "У меня сыну 12 лет, недавно обнаружила, что он смотрит порно, как быть, что делать?", - на сайте Liveexpert.ru был дан следующий ответ:

1. Включите на компе функцию «родительский контроль».

2. Купите и положите ему на стол книгу «Сексуальная энциклопедия для подростков». Это как минимум.

3. Скажите отцу (или дедушке) пусть поговорят с сыном о интересующих мальчика вопросах секса. Здесь не место ханжеству.

Психолог Елена Кузнецова по другому аналогичному вопросу на сайте All-psy.com советует следующее: "Ребенок найдет всю необходимую ему информацию - в интернете ли, от сверстников ли, но найдет обязательно. Так же как любые другие знания о жизни. Особенно заинтересованно будет искать, если почувствует, что родители ведут себя как-то странно: эмоционально подчеркивают особенность темы, называют "для взрослых". У большинства здоровых детей потребности в самих сексуальных отношениях еще нет. Ребенок просто

интересуется сферой. Наиболее разумные родители снимают с темы ажиотаж."

Кстати, на указанных выше сайтах родители могут найти много полезной для себя информации или получить ответ на свой вопрос от квалифицированных психологов.

Простые советы компании ESET - "Как защитить ребенка в сети?"

Создайте «детский» профиль пользователя на вашем ПК или ноутбуке, где будут лишь предназначенные для детей материалы (например, мультфильмы).

Научите ребенка пользоваться социальными сетями и поисковыми сервисами. Заведите ему страничку в соцсетях и адрес электронной почты. Используйте разные пароли!

Используйте настройки безопасности/приватности выбранных сайтов для ограничения доступа к личным данным вашего ребенка.

Проверяйте возрастные ограничения сайтов и видеоигр. Многие из них не предназначены для несовершеннолетних.

Объясните, что в интернете, как и в реальной жизни, не стоит общаться с незнакомыми людьми и тем более раскрывать информацию о себе или семье.

Даже друзьям и знакомым не следует доверять на 100% – профиль одноклассника вашего ребенка может быть взломан злоумышленниками.

Приглядывайте за тем, кого ваш ребенок добавляет в друзья в соцсетях и что публикует в открытом доступе.

Если вашего ребенка в интернете кто-то напугал или расстроил – он должен знать, что в любой момент может прийти к вам и рассказать об этом.

Убедитесь, что в вашей семье компьютеры, ноутбуки и мобильные устройства защищены антивирусным ПО. ESET NOD32 SmartSecurityFamily для пяти устройств – оптимальный выбор.

Активируйте в вашем антивирусном продукте функцию «Родительский контроль» и определите категории сайтов, которые необходимо блокировать (онлайн-магазины, казино, XXX-сайты и др).

Источник информации:
http://www.bizhit.ru/index/informacionnye_ugrozy_v_internete_i_deti/0-457

Составитель: зав. Библиотеки Давлятшина С.Г.

Компьютерный набор и вёрстка: Давлятшина С.Г.

Тираж: 20экз

Библиотека села Рейдово

МБУ Курильской ЦБС

Дети и подростки в Интернете

Современные дети и подростки, которых называют «цифровыми гражданами» легко осваивают компьютер, мобильные устройства и умело пользуются ими. При этом навыки детей в области безопасности в Интернете отстают от их способности осваивать новые приложения и устройства.

Усилия государства и родителей по ограничению доступа к ресурсам, содержащим противоправный контент, не смогут полностью оградить детей от вредной информации. Поэтому необходимо формировать у детей механизмы критической оценки получаемых сведений.

2019г.