ГБУ ДПО СО «Красноярский РЦ»

Безопасность детей в сети Интернет

Автор-составитель:

старший методист

Борисова Н.П.

2016 г.

Оглавление

Интернет — глобальная сеть, объединяющая огромное количество персональных компьютеров по всему миру. Ежедневно более миллиарда людей по всему миру используют Интернет для работы, покупок, поиска информации и развлечений, а также для общения с друзьями и коллегами. Это также хранилище огромного количества информации, изображений и идей. Пользователи могу посещать музеи мирового класса, получать образование, управлять личными финансами и планировать отдых, а также играть в игры, загружать музыку и фильмы, покупать товары и услуги и заводить друзей.

Интернет изменил способ покупки товаров и предоставил новые способы общения. Он сделал дальнюю связь доступнее, а исследования эффективнее. Но преимущества невозможны без рисков. Мир Интернета, как и реальный мир, не избавлен от неприятностей, опасностей и ненадежных людей. Интернет дает новые мощные возможности для связи, покупок и общения. Однако вместе с ним в наши дома проникает и внешний мир.

Обычно, покидая безопасную атмосферу дома и выходя в окружающий мир, мы инстинктивно усиливаем защиту, становясь более подготовленными к возможным опасностям. Вернувшись домой, мы снова снижаем защиту и расслабляемся. Эти действия мы совершаем автоматически, не задумываясь. Однако, безопасность в Интернете требует повышать уровень защиты даже в собственном доме или там, где мы обычно чувствуем себя в безопасности.

Поскольку Интернет превращает компьютер в окно между внешним миром и домом, интернет-безопасность требует использовать средства, контролирующие, кто или что входит в наш дом, и развивающие бдительность: кому стоит доверять, а кому нет.

1. Основные угрозы безопасности компьютера

Основная угроза компьютеру — вредоносные программы: вирусы, программы-черви, программы-трояны и потенциально нежелательные программы, подобные программам-шпионам.

Вирусы

Компьютерные вирусы — программы, специально разработанные для вторжения на компьютер с целью нарушения его работы, а также копирования, повреждения или удаления данных. Эти программы называются вирусами потому, что распространяются на другие компьютеры: в большинстве случаев они требуют для этого некоторых действий пользователя, например щелчка на вложении электронного сообщения.

Компьютерные вирусы могут содержаться в чем-то на первый взгляд интересном, например в развлекательных программах или во вложениях сообщений электронной почты, таких как компьютерные игры, видеоклипы или фотографии. Множество вирусов распространяется случайной рассылкой зараженных электронных сообщений друзьям и коллегам.

Программы-черви

Программы-черви — это более хитроумные вирусы, заражающие другие компьютеры сети автоматически, без участия пользователя. Чтобы заразить другой компьютер, программы-черви захватывают управление определенными программами.

Программы-трояны

Этот тип вирусов, названный в честь троянского коня, маскируется под полезные программы, например игры или антишпионские программы. Попав на компьютер, они могут незаметно уничтожить или похитить ваши данные.

Программы-шпионы

Программы-шпионы отслеживают действия пользователя и отправляют сведения о них своему создателю или совершают какие-либо действия, зависящие от поведения пользователя.

Программы-шпионы могут надоедать всплывающими рекламными окнами, связанными с веб-узлами, которые регулярно посещает пользователь. Они также могут собирать личные сведения или изменять настройки компьютера без ведома пользователя. Программы-шпионы могут даже повредить компьютер или позволить преступникам украсть идентификационные сведения.

Существует множество способов защиты компьютера от вредоносных и потенциально нежелательных программ.

2. Основные угрозы безопасности детей в Интернете

Несомненно, Интернет полезен для детей, однако потенциальные опасности вполне реальны. Узнав больше об этих угрозах, пользователь может избежать опасностей и предотвратить неприятности. Опасности Интернета для детей делятся на пять основных категорий.

Киберхулиганы

В Интернете, как и на любой игровой площадке, одни люди приятны, другие — нет. И дети, и взрослые с помощью Интернета могут изводить или запугивать других людей, начиная с присвоения прозвищ и заканчивая физическими угрозами. Например, дети иногда отправляют угрожающие комментарии или неприличные изображения через службы мгновенных сообщений или блоги, незаметно для родителей и общества бесчестя ребенка.

Злоупотребление обменом файлами

Обмен музыкой, видео и другими файлами рискован. Дети случайно могут загрузить неуместные материалы, компьютерные вирусы или программы-шпионы. Некоторые программы для обмена файлами дают доступ к компьютеру в любое время, пока он в сети.

Доступ к неприличному контенту

Дети зачастую не в силах противостоять любопытству. Пользуясь Интернетом, они могут столкнуться с информацией или изображениями, доступ к которым родители хотели бы ограничить, например, с контентом неприличного характера, недопустимым для детей или не соответствующим ценностям семьи. Это может случиться при нажатии на рекламные или непонятные ссылки на поисковой странице либо при обмене файлами через Интернет

Киберхищники

Киберхищники используют Интернет для сближения с детьми. Их цель — изолировать детей и убедить их встретиться лично. О людях в сети известно только то, что они сами сообщают о себе. Киберхищники пользуются этой анонимностью для обмана детей, притворяясь другим ребенком или кем-то еще, кто заслуживает доверия. Эти люди могут также использовать подростковые стремления к приключениям и романтике, чтобы завязать с ними недопустимые дружеские отношения.

Вторжение в частную жизнь

Некоторые организации используют регистрацию или формы опроса для сбора личных сведений. При заполнении различных форм в Интернете без присмотра дети могут предоставить конфиденциальные сведения о себе или Вашей семье. Дети также могут случайно предоставить личные сведения или фотографии в блогах, на персональных веб-страницах или при игре через Интернет.

3. Кибербуллинг

Кибербуллинг сегодня – это уже проблема глобального масштаба, и она активно набирает темп! Чтобы эффективно бороться с разными видами травли в сети, необходимо уметь определять их.

«Кибербуллингом называется использование силы или влияния, прямо или косвенно, в устной, письменной или физической форме, либо путем демонстрации или иного использования снимков, символов или чего-либо другого в целях запугивания, угроз, травли, преследования или смущения при помощи интернета или других технологий, к примеру, мобильных телефонов.» Дэвид Фэйган, юрист, BizLegal.eu

1. Исключение

Эта форма кибербуллинга аналогична бойкоту: жертву намеренно исключают из отношений и коммуникации. При этом возможны самые разнообразные проявления исключения:

Вашего ребенка могут не допускать к играм, встречам или другим совместным занятиям с его друзьями.

Друзья вашего ребенка могут не допускать его к совместным разговорам онлайн.

Иногда причинами к исключению может быть то, что у ребенка нет смартфона, или же то, что он не пользуется социальными сетями.

2. Домогательство

Домогательством называют постоянную и умышленную травлю при помощи оскорбительных или угрожающих сообщений, отправленных вашему ребенку лично или как часть какой-либо группы.

Эта форма кибербуллинга крайне опасна и может привести к серьезным последствиям для вашего ребенка. Эти злонамеренные сообщения могут устрашить ребенка и навредить ему, делая его неуверенным в себе. То, что такие сообщения будут посылаться постоянно, означает, что ребенку не будет даваться никакой передышки от травли, что делает этот вид кибербуллинга особенно опасным.

3. Аутинг

Аутингом называется преднамеренная публикация личной информации ребенка с целью его унизить, при этом произведенная без его согласия.

Аутинг может принимать разные формы, при этом опубликованная информация может быть как серьезной, так и незначительной. Даже чтение сохраненных сообщений на телефоне вашего ребенка можно считать аутингом. Личную информацию никогда нельзя разглашать, поэтому вы должны обязательно убедиться, что, если такой случай произойдет с вашим ребенком, он сообщит о кибербуллинге представителям социальной сети, школы или другого учреждения в соответствии с конкретной ситуацией.

4. Киберсталкинг

Киберсталкинг может привести к тому, что киберобидчик – человек, который производит саму травлю, – будет представлять реальную угрозу для безопасности и благополучия вашего ребенка. В частности, этим термином могут называться попытки взрослых связаться с детьми и подростками через Интернет с целью личной встречи и дальнейшей сексуальной эксплуатации. Эта форма кибербуллинга крайне опасна и может иметь самые серьезные последствия, поэтому по обнаружению необходимо принимать все меры, чтобы немедленно ее остановить.

5. Фрейпинг

Фрейпингом называют форму кибербуллинга, в которой обидчик каким-либо образом получает контроль над учетной записью вашего ребенка в социальных сетях и публикует нежелательный контент от его имени.

Несмотря на то, что некоторые могут считать это занятие забавным и смешным, фрейпинг – серьезное преступление, которое может привести к серьезным последствиям. Так можно полностью разрушить репутацию жертвы – важно помнить, что Google никогда ничего не забывает. Если что-то было опубликовано в сети, то в какой-то форме оно там останется навсегда.

6. Поддельные профили

Киберобидчики могут создавать поддельные профили – скрывать то, кем они на самом деле являются, чтобы травить вашего ребенка.

Также они могут использовать чужие телефонные номера и адреса электронной почты, чтобы заставить вашего ребенка думать, что им угрожает не обидчик, а кто-то другой. Часто хулиганы используют поддельные профили, потому что боятся, что их личность станет известна. Такое обычно бывает, когда обидчик – кто-то, кого ваш ребенок хорошо знает.

7. Диссинг

Диссингом называют передачу или публикацию порочащей информации о жертве онлайн. Это делается с целью испортить репутацию жертвы или навредить ее отношениям с другими людьми.

Информация может публиковаться в самых разных форматах, от текста до фото, скриншотов или видео. Обидчик всеми силами будет пытаться унизить вашего ребенка, при этом привлекая максимум внимания к этому процессу. В этом случае обидчик чаще всего кто-то из знакомых вашего ребенка, что может дополнительно усугубить ситуацию.

8. Обман

В этом случае киберхулиган обманом пытается завоевать доверие вашего ребенка, чтобы тот рассказал ему какую-либо чувствительную информацию, которую обидчик затем публикует в сети.

Обидчик сперва «подружится» с вашим ребенком и обманом вызовет у него ложное чувство безопасности, а потом нарушит созданное доверие и отправит полученную информацию третьим лицам.

9. Троллинг

Троллингом называют намеренную провокацию при помощи оскорблений или некорректной лексики на интернет-форумах и в социальных сетях.

Тролли будут лично нападать на жертву и стараться унизить ее. Основная задача троллинга – разозлить жертву и заставить ее прибегнуть, так же как и сам тролль, к оскорблениям и некорректной лексике. Тролли могут тратить долгое время в поисках особенно уязвимой жертвы. Как правило, тролли получают положительные эмоции за счет унижения других.

10. Кетфишинг

Кетфишинг – форма кибербуллинга, в которой киберхулиган с целью обмана воссоздает профили жертвы в социальных сетях на основе украденных фотографий и других личных данных.

Чаще всего обидчики будут пытаться скрыть, кем они на самом деле являются. Они будут использовать информацию, которую ваш ребенок уже разместил в социальных сетях, для создания поддельных личностей. Иногда они ограничатся только фотографией вашего ребенка и используют выдуманное имя, но иногда они могут использовать и всю доступную информацию. Часто бывает сложно понять, зачем обидчик занимается кетфишингом, но в любом случае важно понимать, что эта форма кибербуллинга может серьезно навредить репутации вашего ребенка.

Основные признаки жертвы кибербуллинга

1. Изменения в настроении

Вы заметили, что человек стал грустнее?

Он старается избегать общественных мероприятий?

Наблюдаются изменения в его поведении, особенно в отношении к интернету?

Он стал использовать свои мобильные устройства не так часто, как раньше? Реагирует ли он негативно на звук нового сообщения его телефона?

Любое резкое изменение в настроении человека, сохраняющееся продолжительное время, может оказаться признаком того, что человек подвергается кибербуллингу. Такое изменение, конечно, может быть и признаком других проблем, однако выявить кибербуллинг довольно просто, и можно исключить его в первую очередь. Просто поговорите с этим человеком, выбирая как можно более дружественные и менее осуждающие тона.

2. Напуганность

Есть ли признаки того, что человек напуган чем-либо? Он:

Боится идти в школу?

Боится принимать участие в общественных мероприятиях?

Боится посещать занятия в спортивной или любой иной секции?

Боится пользоваться интернетом?

Боится сигналов своего мобильного телефона?

Страх – всегда достаточная причина для беспокойства, и то, что человек часто напуган, может быть признаком кибербуллинга. Как и в предыдущем случае, это может оказаться и признаком других проблем, поэтому имеет смысл постараться исключить кибербуллинг в первую очередь, как более простую в распознании проблему.

3. Удаление страниц в социальных сетях

Человек, который подвергается кибербуллингу, может удалить свои страницы в социальных сетях, чтобы избежать травли. Если вы знаете кого-то, кто в последнее время

внезапно удалил свои страницы в социальных сетях, не объяснив, почему, – поговорите с ним, возможно он пытается таким образом защитить себя от травли.

4. Оскорбительные или унизительные изображения и сообщения в сети

Кибербуллинг может происходить на глазах у всех, поэтому и вы, возможно, сможете увидеть в общем доступе и сообщения, направленные кому-то из ваших друзей или знакомых.

4. Основные угрозы личной безопасности в Интернете

Множество полезных и приятных сервисов Интернета требуют делиться сведениями о себе. Одни требует совсем немного, другие больше. Не всегда легко понять, кто и зачем собирает эту информацию.

Иногда предоставление сведений приносит непредвиденные и нежелательные результаты. Эти результаты могут просто раздражать (например, нежелательные сообщения электронной почты) или быть чем-то серьезным, например попыткой кражи идентификационных сведений, нанесением ущерба репутации, а также попыткой кражи денег.

Кража идентификационных сведений и интернет-мошенничество

Интернет-мошенники хотят, чтобы вы отдали им с трудом заработанные деньги или предоставили личные сведения, которые позволят им украсть Ваши идентификационные сведения. Преступники давно поняли, что Интернет может помочь им обманывать доверчивых людей, иногда весьма изощренными методами. Большинство афер в Интернете основано на мошенничестве и краже идентификационных сведений — и лишь от пользователя зависит, предоставлять или нет личные сведения, отправлять деньги или нет. Таким образом, зная, на что обращать внимание и что делать, Вы не станете жертвой этих преступлений.

Фишинг

Чрезвычайно подлое мошенничество, известное как фишинг, начинается с сообщения электронной почты от источника, которому доверяет пользователь. Поддельное сообщение электронной почты — «наживка» — обычно содержит ссылку на поддельную веб-страницу, очень похожую на страницу компании, которой доверяют. Этот веб-узел может запросить личные сведения, например номер кредитной карты. Это «крючок». Если пользователь заглотил крючок — он попал в неприятности, потому что предоставил преступникам достаточно сведений для кражи идентификационных сведений и получения доступа к своим учетным записям, деньгам или счетам.

Мистификация

Мистификация — еще один тип мошенничества. Например, «нигерийское мошенничество» — тип авансового мошенничества, долгое время пользовавшийся «популярностью». Жертва получала сообщение электронной почты от кого-либо, выдающего себя за нигерийского чиновника, деловую персону или выжившего супруга прежнего лидера правительства, просящего помощи в вывозе денег из страны. Мошенники, отправившие это сообщение, предлагали перечислить на банковский счет жертвы миллионы долларов в обмен на небольшое вознаграждение. Если жертва отвечала на первое письмо, мошенники могли прислать официально выглядящие документы или другие «доказательства» и просьбу предоставить чистый фирменный бланк, номера банковских счетов и как можно больше денег, чтобы покрыть затраты на перевод и судебные издержки. Если жертва продолжала отвечать, мошенники предоставляли дополнительные «свидетельства», подтверждавшие их намерения, и тревога поднималась только, когда мошенники запрашивали больше денег и задерживали перевод обещанной суммы на счет жертвы. В конечном счете мошенники исчезали с деньгами жертвы, оставляя ее с носом.

Другой известный мистификатор предлагал жертве купить билеты международной лотереи и использовать «секретную систему» для выигрыша большой суммы денег. Или посылал сообщение электронной почты, извещающее получателя об огромном выигрыше в международную лотерею, даже если он не участвовал в ней, требующее только номер его

банковского счета, чтобы перечислить выигрыш. Конечно же, не было никакой «секретной системы», а большинство лотерей, упомянутых в этих сообщениях, были вымышленными.

Нежелательная почта

Один из инструментов, используемых мошенниками и преступниками — нежелательная почта, то есть сообщения электронной почты, мгновенные сообщения и даже электронные поздравительные открытки, которые Вы не запрашивали. Нежелательная почта может содержать ссылки на поддельные веб-узлы или рекламные объявления о бесполезных продуктах, в которых Вы не заинтересованы.

Необходимые шаги для безопасности в Интернете — внимательность, здравый смысл и умение распознавать жульничество и интернет-мошенничество и избегать их.

5. Онлайн шантаж

В последнее время и СМИ и органы правопорядка все больше обращают внимание на онлайн-шантаж с помощью откровенных фотографий, называющийся в английском языке словом sextortion. Суть этого явления проста — злоумышленник добывает фотографии или видео, изображающие интимную жизнь своей будущей жертвы, а затем шантажирует, угрожая распространением этих материалов. Чаще всего, целью шантажа является получение новых снимков или видео. Такой вот замкнутый круг.

Зачастую злоумышленники получают снимки, взламывая плохо защищенные аккаунты, или заражая устройства вредоносными программами. В результате они получают доступ к галереям или облачным хранилищам своих жертв, а в некоторых случаях и к их веб-камерам. Впрочем, случается что жертва сама отправляет злоумышленнику снимки, поддавшись на его уловки.

К сожалению, это неприятное явление имеет самое прямое отношение к детской онлайн-безопасности. Старший научный сотрудник Брукинского института Бенджамин Уитс (Benjamin Wittes) изучил 78 уголовных дел, в которых фигурировало порядка 3000 жертв и обнаружил, что подавляющее большинство — 78% — всех жертв были несовершеннолетними. Если задуматься, в этом нет ничего удивительного: получить доступ к аккаунту подростка проще — они реже используют двухфакторную аутентификацию, придумывают более очевидные пароли, меньше осведомлены о правилах онлайн-безопасности. Кроме того, в подростковой среде очень распространен секстинг — отправка сообщений интимного характера. Так, по данным The National Campaign, 20% тинейджеров делятся своими обнаженными фотографиями. Почти 40% размещают сообщения непристойного содержания. 15% из тех, кто отправлял кому-либо фото без одежды, признались, что делились ими с людьми, которых не знали в реальном мире — только в Сети.

При этом, ребенок зачастую стыдится рассказать родителям о факте вымогательства, опасаясь наказания или непонимания с их стороны. Таким образом подросток оказывается в неприятной безвыходной ситуации, которая потенциально может нанести ему глубокую психологическую травму. СМИ даже рассказывали о случаях самоубийства в результате сексуального вымогательства.

Для того, чтобы не попасть в сложную ситуацию самим и обезопасить детей от сексуального вымогательства надо соблюдать **несколько простых правил цифровой гигиены**:

- ✓ Помните об элементарных средствах онлайн-защиты — разумное поведение в сети и проверенный антивирус с актуальными базами защитит от перехвата управления вашим компьютером.
- ✓ Никогда не делайте, не отправляйте и не храните на своих устройствах, или в облачных хранилищах свои интимные фотографии. Помните, что к снимкам может получить доступ злоумышленник, без вашего ведома, например, взломав ваш аккаунт, или аккаунт того человека, которому вы отправили снимки. Безопаснее будет, если таких снимков в вашей биографии вовсе не будет существовать.
- ✓ Двухфакторная аутентификация и надежный пароль важны не меньше антивируса для защиты вашей цифровой собственности. Даже если вы не храните интимных фотографий в своих аккаунтах, там все равно наверняка есть информация, которую вы бы не хотели потерять.
- ✓ Избегайте общения с незнакомыми в реальности людьми по неанонимным каналам связи (социальным сетям, мессенджерам). Не раскрывайте своего инкогнито в переписке с виртуальными знакомыми. Отслеживайте, с кем общаются ваши дети по таким каналам связи, чтобы поднять тревогу в случае начавшихся частых контактов с подозрительным, на ваш взгляд, человеком. Это можно сделать при помощи специализированного программного обеспечения
- ✓ Расскажите детям о сексуальном вымогательстве и перечисленных правилах. Говорить с детьми на такие темы бывает трудно, но подросток должен знать, какие последствия могут ждать его в результате необдуманных действий в сети.

6. Детский интернет

Сейчас дети с очень раннего возраста начинают пользоваться не только различными гаджетами, но и Интернетом. Все больше людей склоняются к тому, что Сеть может принести ребенку много пользы, а вред можно минимизировать с помощью специального ПО и правильного воспитания.

В этой связи все чаще звучат слова «детский Интернет». Говоря о детском Интернете, подразумевается вся совокупность различных детских страничек: детские поисковики, детские социальные сети, игровые и образовательные сайты для детей и иногда даже сайты детских

интернет-магазинов. Для разных возрастов подходят разные наборы сайтов. По наблюдениям специалистов, их интересы таковы.

0–4 года

В этом возрасте еще рано говорить об интернет-серфинге. Малышам интересны игры, аудиосказки, мультики, интерактивные книги. Все это он может использовать и не выходя в Интернет — родители могут скачать и установить все, что посчитают необходимым.

Возможно, родителям детей такого возраста будут интересны сайты, с которых можно скачать и распечатать настоящие бумажные раскраски. Таких в Интернете множество, и они легко ищутся поисковиками.

4–6 лет

Дошкольники делают свои первые шаги в Интернете в поиске развлечений. Им будут интересны сайты с играми, интерактивными раскрасками, детские аудиокниги, мультики. В общем, все то, что родители устанавливали для них и раньше. Только теперь им будет интересно найти и выбрать что-то новое самостоятельно.

Детских сайтов, отвечающих запросам этой возрастной группы, в Интернете, пожалуй, больше всего.

6–11 лет

С одной стороны, младшим школьникам будут интересны все те же сайты, что и дошколятам. С другой — сфера их интересов расширяется, им становятся интересны более взрослые игры и книги, они начинают использовать Интернет для учебы и самообразования.

С развлекательными сайтами никаких проблем нет — тут можно использовать и уже освоенные в более младшем возрасте сайты, и новые, ориентированные именно на эту группу. А вот с интересными сайтами для учебы все не так однозначно: в некоторых странах найти их не сложнее, чем развлекательные, а в других — не отыщешь днем с огнем.

11–16 лет

На первый план у подростков выходит, конечно же, общение. Ограничивать ребенка такого возраста рамками детского Интернета становится все сложнее, поскольку его потребности уже выходят за пределы того, что может быть предложено детскими сайтами.

На данном этапе рекомендуется начинать переход к взрослому Интернету. Необходимо использовать настройки программ родительского контроля, чтобы оградить ребенка от сайтов, содержание которых ему не подходит.

7. Рекомендации для родителей

Дети и подростки — активные пользователи интернета. С каждым годом сообщество российских интернет-пользователей молодеет. Дети поколения Рунета растут в мире, сильно отличающемся от того, в котором росли их родители. Одной из важнейших координат их развития становятся инфо-коммуникационные технологии и, в первую очередь, интернет. Между тем, помимо огромного количества возможностей, интернет несет и множество рисков. Зачастую дети и подростки в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети. Сделать их пребывание в интернете более безопасным, научить их ориентироваться в киберпространстве — важная задача для их родителей.

Основные правила безопасности для родителей

- ✓ Прежде, чем позволить ребенку пользоваться Интернетом, расскажите ему о возможных опасностях Сети (вредоносные программы, небезопасные сайты, интернет-мошенники и др.) и их последствиях.
- ✓ Четко определите время, которое Ваш ребенок может проводить в Интернете, и сайты, которые он может посещать.
- ✓ Убедитесь, что на компьютерах установлены и правильно настроены антивирусные программы, средства фильтрации контента и нежелательных сообщений.

- ✓ Контролируйте деятельность ребенка в Интернете с помощью специального программного обеспечения.
- ✓ Спрашивайте ребенка о том, что он видел и делал в Интернете.
- ✓ Объясните ребенку, что при общении в Интернете (чаты, форумы, сервисы мгновенного обмена сообщениями, онлайн-игры) и других ситуациях, требующих регистрации, нельзя использовать реальное имя. Помогите ему выбрать регистрационное имя, не содержащее никакой личной информации.
- ✓ Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также "показывать" свои фотографии.
- ✓ Помогите ребенку понять, что далеко не все, что он может прочесть или увидеть в Интернете — правда. Приучите его спрашивать то, в чем он не уверен.
- ✓ Объясните ребенку, что нельзя открывать файлы, полученные от неизвестных пользователей, так как они могут содержать вирусы или фото/видео с негативным содержанием.
- ✓ Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации.
- ✓ Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека.
- ✓ Постараться регулярно проверять список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются;
- ✓ Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов — читать грубости также неприятно, как и слышать;
- ✓ Проверяйте актуальность уже установленных правил. Следите за тем, чтобы Ваши правила соответствовали возрасту и развитию Вашего ребенка.

8. Словарь интернет-угроз

Аутинг - преднамеренная публикация личной информации ребенка с целью его унизить, при этом произведенная без его согласия. Аутинг может принимать разные формы, при этом опубликованная информация может быть как серьезной, так и незначительной. Даже чтение сохраненных сообщений на телефоне ребенка можно считать аутингом. Личную информацию никогда нельзя разглашать, поэтому родители должны обязательно убедиться, что, если такой случай произойдет с ребенком, он сообщит о кибербуллинге представителям социальной сети, школы или другого учреждения в соответствии с конкретной ситуацией.

Вирусы (Viruses): программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение. Скорость распространения вирусов несколько ниже, чем у червей.

Вишинг назван так по аналогии с фишингом — распространённым сетевым мошенничеством. Сходство названий подчеркивает тот факт, что принципиальной разницы между вишингом и фишингом нет. Основное отличие вишинга в том, что так или иначе задействуется телефон. Типичный пример фишинга, когда клиенты какой-либо платёжной системы получают сообщения по электронной почте якобы от администрации или службы безопасности данной системы с просьбой указать свои счета, пароли и т.п. При этом ссылка в сообщении ведёт на поддельный сайт, на котором и происходит кража информации. Сайт этот уничтожается через некоторое время, и отследить его создателей в интернете достаточно сложно.

Вредоносные программы — различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт-диски, флешки и т.д.), но и через электронную почту посредством спама или скачанных из интернета файлов.

Гриферство или грифинг — акт нанесения морального и материального ущерба людям в компьютерных играх. Иными словами, это внутриигровой вандализм.

Груминг – это установление дружеского и эмоционального контакта с ребенком в интернете для его дальнейшей сексуальной эксплуатации. Работают преступники по следующей схеме: лицо, заинтересованное в интимной связи с несовершеннолетним, представляется в сети другим человеком, втирается в доверие к ребенку и настаивает на личной встрече. Последствия для поддавшегося на уговоры ребенка могут быть очень плачевны.

Диссинг - передача или публикация порочащей информации о жертве онлайн. Это делается с целью испортить репутацию жертвы или навредить ее отношениям с другими людьми. Информация может публиковаться в самых разных форматах, от текста до фото, скриншотов или видео. Обидчик всеми силами будет пытаться унизить ребенка, при этом привлекая максимум внимания к этому процессу.

Домогательство - постоянная и умышленная травля при помощи оскорбительных или угрожающих сообщений, отправленных вашему ребенку лично или как часть какой-либо группы. Эта форма кибербуллинга крайне опасна и может привести к серьезным последствиям для ребенка. Эти злонамеренные сообщения могут устрашить ребенка и навредить ему, делая его неуверенным в себе. То, что такие сообщения будут посылаться постоянно, означает, что ребенку не будет даваться никакой передышки от травли, что делает этот вид кибербуллинга особенно опасным.

Интернет-зависимость — навязчивое желание войти в интернет, находясь офлайн и неспособность выйти из интернета, будучи онлайн. По своим проявлениям она схожа с уже известными формами аддиктивного поведения (например, в результате употребления алкоголя или наркотиков), но относится к типу нехимических зависимостей, то есть не приводящих непосредственно к разрушению организма. По своим симптомам интернет-зависимость ближе к зависимости от азартных игр; для этого состояния характерны следующие признаки: потеря ощущения времени, невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером, досада и раздражение при невозможности выйти в интернет. Исследователи отмечают, что большая часть Интернет-зависимых (91 %) пользуется сервисами Интернета, связанными с общением. Другую часть зависимых (9%) привлекают информационные сервисы сети.

Исключение - форма кибербуллинга аналогична бойкоту: жертву намеренно исключают из отношений и коммуникации.

Кетфишинг – форма кибербуллинга, в которой киберхулиган с целью обмана воссоздает профили жертвы в социальных сетях на основе украденных фотографий и других личных данных. Чаще всего обидчики будут пытаться скрыть, кем они на самом деле являются. Они будут использовать информацию, которую ребенок уже разместил в социальных сетях, для создания поддельных личностей. Иногда они ограничатся только фотографией ребенка и

используют выдуманное имя, но иногда они могут использовать и всю доступную информацию. Часто бывает сложно понять, зачем обидчик занимается кетфишингом, но в любом случае важно понимать, что эта форма кибербуллинга может серьезно навредить репутации ребенка.

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов. Английское слово буллинг (bullying, от bully — драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. Основной площадкой для кибербуллинга в последнее время являются социальные сети. В них можно оскорблять человека не только с помощью сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унизительный контент.

Кибербуллинг- использование силы или влияния, прямо или косвенно, в устной, письменной или физической форме, либо путем демонстрации или иного использования снимков, символов или чего-либо другого в целях запугивания, угроз, травли, преследования или смущения при помощи интернета или других технологий, к примеру, мобильных телефонов.

Кибермошенничество — один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.). Отправка любых смс на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.

Киберпреследование - это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование.

Кибersталкинг - этим термином могут называться попытки взрослых связаться с детьми и подростками через Интернет с целью личной встречи и дальнейшей сексуальной эксплуатации. Эта форма кибербуллинга крайне опасна и может иметь самые серьезные последствия, поэтому по обнаружению необходимо принимать все меры, чтобы немедленно ее остановить.

Контентные риски - материалы (тексты, картинки,аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. В первую очередь, с таким контентом можно столкнуться на сайтах социальных сетей, в блогах, на торрентах. Но сегодня практически весь интернет - это виртуальное пространство риска.

Незаконный контакт — это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка. Это понятие включает в себя такие интернет-преступления как домогательство и груминг.

Незаконный контент - распространение наркотических веществ через интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям.

Неэтичный контент - контент, который не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей. Подобное содержимое может распространяться ограниченно (например, "только для взрослых"). Особо опасны сайты, на

которых обсуждаются способы причинения боли и вреда, способы чрезмерного похудения, способы самоубийства, сайты, направленные против отдельных групп или лиц. Столкновения с контентными рисками могут иметь негативные последствия для эмоциональной сферы психологического развития, социализации, а также физического здоровья детей и подростков.

Нигери́йские пи́сьма — распространённый вид мошенничества, получивший наибольшее развитие с появлением массовых рассылок по электронной почте (спама). Письма названы так потому, что особое распространение этот вид мошенничества получил в Нигерии, причём ещё до распространения Интернета, когда такие письма распространялись по обычной почте. Однако нигерийские письма приходят и из других африканских стран, а также из городов с большой нигерийской диаспорой (Лондон, Амстердам, Мадрид, Дубай). Рассылка писем началась в середине 1980-х гг. Как правило, мошенники просят у получателя письма помощи в многомиллионных денежных операциях, обещая солидные проценты с сумм. Если получатель согласится участвовать, у него постепенно выманиваются все более крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам, и т. п..

Обман - киберхулиган обманом пытается завоевать доверие ребенка, чтобы тот рассказал ему какую-либо чувствительную информацию, которую обидчик затем публикует в сети. Обидчик сначала «подружится» с ребенком и обманом вызовет у него ложное чувство безопасности, а потом нарушит созданное доверие и отправит полученную информацию третьим лицам.

Онлайн-шантаж — злоумышленник добывает фотографии или видео, изображающие интимную жизнь своей будущей жертвы, а затем шантажирует, угрожая распространением этих материалов. Чаще всего, целью шантажа является получение новых снимков или видео. Такой вот замкнутый круг. Зачастую злоумышленники получают снимки, взламывая плохо защищенные аккаунты, или заражая устройства вредоносными программами. В результате они получают доступ к галереям или облачным хранилищам своих жертв, а в некоторых случаях и к их веб-камерам. Впрочем, случается что жертва сама отправляет злоумышленнику снимки, поддавшись на его уловки. При этом, ребенок зачастую стыдится рассказать родителям о факте вымогательства, опасаясь наказания или непонимания с их стороны. Таким образом подросток оказывается в неприятной безвыходной ситуации, которая потенциально может нанести ему глубокую психологическую травму.

Поддельные профили - киберобидчики могут создавать поддельные профили – скрывать то, кем они на самом деле являются, чтобы травить ребенка. Также они могут использовать чужие телефонные номера и адреса электронной почты, чтобы заставить ребенка думать, что им угрожает не обидчик, а кто-то другой. Часто хулиганы используют поддельные профили, потому что боятся, что их личность станет известна.

Потенциально опасные приложения (Riskware): программное обеспечение, не являющееся вирусом, но содержащее в себе потенциальную угрозу. При некоторых условиях наличие таких программ на компьютере подвергает ваши данные риску. К таким программам относятся утилиты удаленного администрирования, программы автоматического дозвона на платные ресурсы интернета с использованием Dial Up-соединения и другие.

Программы-маскировщики (Rootkit): это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Rootkit'ы также могут модифицировать операционную систему на компьютере и заменять основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Программы-рекламы (Adware): программный код, без ведома пользователя включенный в программное обеспечение с целью демонстрации рекламных объявлений. Как правило,

программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе.

Программы-шпионы: программное обеспечение, позволяющее собирать сведения об отдельно взятом пользователе или организации без их ведома. О наличии программ-шпионов на своем компьютере вы можете и не догадываться. Как правило, целью программ-шпионов является: отслеживание действий пользователя на компьютере; сбор информации о содержании жесткого диска; в этом случает чаще всего речь идет о сканировании некоторых каталогов и системного реестра с целью составления списка программного обеспечения, установленного на компьютере; сбор информации о качестве связи, способе подключения, скорости модема и т.д. Однако данные программы не ограничиваются только сбором информации, они представляют реальную угрозу безопасности. Как минимум две из известных программ – Gator и eZula – позволяют злоумышленнику не просто собирать информацию, но и контролировать чужой компьютер. Другим примером программ-шпионов являются программы, встраивающиеся в установленный на компьютере браузер и перенаправляющие трафик. Наверняка вы встречались с подобными программами, если при запросе одного адреса веб-сайта открывался совсем другой.

Программы-шутки (Jokes): программное обеспечение, не причиняющее компьютеру какого-либо прямого вреда, но выводящее сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях. Такие программы часто предупреждают пользователя о несуществующей опасности, например, выводят сообщения о форматировании диска (хотя никакого форматирования на самом деле не происходит), обнаруживают вирусы в незараженных файлах и т.д.

Прочие опасные программы: разнообразные программы, которые разработаны для создания других вредоносных программ, организации DoS-атак на удаленные сервера, взлома других компьютеров и т. п. К таким программам относятся хакерские утилиты (Hack Tools), конструкторы вирусов и т.д.

Секстинг - отправление сообщений интимного характера. Это может быть просто текстовая переписка, фотографии или видео. Преступники находят контакты подростка и связываются с ним, чтобы получить эротические фотографии или видео. Фото или видео можно отправить через любой мессенджер или социальную сеть. Это позволяет получать от детей интимные снимки, не вступая с ними в контакт в реальной жизни. Помимо прочего злоумышленники зачастую неплохо понимают детскую психологию и могут убедить ребенка, что все, что он делает, якобы безобидно. Такие фото и видеоматериалы могут стать частью «личной коллекции» педофила, но гораздо чаще они оказываются на ресурсах, распространяющих детскую порнографию. Борьба с сайтами, содержащими детскую порнографию, ведется давно и активно, и найти их в открытом доступе сейчас очень сложно. Тем не менее, это не означает, что они исчезли. Детская порнография остается одним из направлений криминального бизнеса и, очевидно, приносит производителям контента немалые деньги.

Спам (Spam): анонимная, массовая почтовая корреспонденция нежелательного характера. Так, спамом являются рассылки политического и агитационного характера, письма, призывающие помочь кому-нибудь. Отдельную категорию спама составляют письма с предложениями обналичить большую сумму денег или вовлекающие в финансовые пирамиды, а также письма, направленные на кражу паролей и номеров кредитных карт, письма с просьбой переслать знакомым (например, письма счастья) и т. п. Спам существенно повышает нагрузку на почтовые сервера и повышает риск потери информации, важной для пользователя.

Троллинг - намеренная провокация при помощи оскорблений или некорректной лексики на интернет-форумах и в социальных сетях. Тролли будут лично нападать на жертву и стараться

унизить ее. Основная задача троллинга – разозлить жертву и заставить ее прибегнуть, так же как и сам тролль, к оскорблениям и некорректной лексике. Тролли могут тратить долгое время в поисках особенно уязвимой жертвы. Как правило, тролли получают положительные эмоции за счет унижения других.

Троянские программы (Trojans): программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к "зависанию", воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом "полезного" программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

Фарминг — один из видов сетевого мошенничества, похожий на фишинг и основанный на использовании фальшивых веб-сайтов и краже конфиденциальной информации. Отличие фарминга от фишинга заключается в следующем: в аферах с фишингом пользователь переходит на фиктивный веб-сайт, попадаясь на уловку в виде фальшивого электронного письма или ссылки, в то время как фарминг работает за счет перенаправления жертв на фиктивный веб-сайт даже тогда, когда пользователь ввел правильный веб-адрес. Чаще всего это происходит с веб-сайтами банков или интернет-магазинов.

Фишинг (Phishing) – почтовая рассылка, целью которой является получение от пользователя конфиденциальной информации как правило финансового характера. Такие письма составляются таким образом, чтобы максимально походить на информационные письма от банковских структур, компаний известных брендов. Письма содержат ссылку на заведомо ложный сайт, где пользователю предлагается ввести, например, номер своей кредитной карты и другую конфиденциальную информацию.

Флейминг — «спор ради спора», процесс обмена сообщениями в местах многопользовательского сетевого общения (чаты, Интернет-форумы, социальные сети и др.). Данное явление представляет собой словесную войну, которая зачастую не имеет отношения к первоначальной причине дискуссии, спора. Иногда применяется в контексте троллинга, но чаще всего флейм вспыхивает из-за недоразумения, обиды на виртуального собеседника.

Фрейпинг - форма кибербуллинга, в которой обидчик каким-либо образом получает контроль над учетной записью ребенка в социальных сетях и публикует нежелательный контент от его имени.

Черви (Worms): данная категория вредоносных программ для распространения использует сетевые ресурсы. Название этого класса было дано исходя из способности червей "переползать" с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Также благодаря этому черви обладают исключительно высокой скоростью распространения. Черви проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Использованные интернет-ресурсы:

1. Защита детей https://kids.kaspersky.ru/

2. Дети онлайн http://detionline.com/helpline/rules/parents

3. Родителям об информационной безопасности
https://sites.google.com/site/roditelidetibezogfsnost/kommunikacionnye-riski/kiberpresledovanie

4. Википедия https://ru.wikipedia.org

5. Norton by Symantec https://ru.norton.com/cybercrime-pharming/

6. Лаборатория Касперского https://support.kaspersky.ru/614