Российская Федерация
Иркутская область
МУНИЦИПАЛЬНОЕ КАЗЁННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ШЕЛЕХОВСКОГО РАЙОНА
«НАЧАЛЬНАЯ ШКОЛА – ДЕТСКИЙ САД № 14»
(МКОУ ШР «НШДС № 14»)

Как обезопасить ребенка

в современном информационном обществе.

Разработали:
Сильванович И.Л.,
социальный педагог
89027665479
Панова А.К.,
учитель информатики.
89501442093

Шелехов 2024г.

Актуальность мероприятия:

Современные средства коммуникации стали неотъемлемой частью повседневной жизни людей и опосредуют практически все сферы человеческой деятельности. Число пользователей интернета неуклонно растет с каждым днем, а самыми активными среди них являются молодые люди, подростки и дети.

Дети проводят в сети гораздо больше времени, чем хотелось бы многим родителям. Большинство родителей не всегда могут найти время, чтобы следить за действиями детей в интернете.

Это напряженное время для родителей, которые хотят защитить своих детей. Недавнее исследование «Лаборатории Касперского» демонстрирует масштаб проблемы. Вот что происходит с сегодняшней молодежью:

- 73% подростков не представляют жизни без смартфонов, а половина из них берут с собой телефон, когда ложатся спать.
- 44% детей в возрасте от 8 до 16 лет постоянно находятся в сети, предпочитая приложения для развлечения и социальные сети.
- 40% детей раскрывают в интернете конфиденциальную информацию, включая домашний адрес.
- Треть молодых людей сообщают в интернете неверную информацию о своем возрасте.
- 37% детей сталкивались с опасностями в интернете, включая кибербуллинг, финансовые угрозы и неприемлемый контент.

Ни один родитель не сможет отследить все, что ребенок делает на своем смартфоне и ноутбуке.

При регистрации на платформе СФЕРУМ, многие родители не подозревали, что их ребенок уже зарегистрирован ВКонтакте (регистрация с 18 лет).

Почему ребенок тянется в интернет-пространство? Что именно его манит в сети как магнитом? Почему многие родители, с одной стороны – также подвержены веяниям современности и владеют навыками общения в сети, с другой стороны – совершенно не осведомлены, чем их ребенок занимается в интернете? Почему всё чаще СМИ освещает страшные, необратимые случаи детских суицидов, экстремистской деятельности подростков? Почему дети не справляются со своими проблемами и ищут решение не в семье, не в школе, а в интернете? Действительно ли всемирная сеть – средоточие всех проблем современного мира? Или это всего лишь ширма, повод, а настоящие проблемы таятся, как и много лет назад именно в семье, живом общении, школе? Эти вопросы именно сегодня актуальны, как никогда. Именно сегодня эта проблема стоит наиболее остро как на законодательном уровне, так и в каждой отдельно взятой семье.

Что могут и должны сделать родители для своих детей, чтобы не допустить рокового шага?

«Проектная задача» - это система заданий (действий), направленных на поиск лучшего пути достижения результата в виде реального «продукта»

Новизна занятия:

Социальные сети и мессенджеры развиваются и растут с геометрической прогрессией. Еще несколько лет назад никто не мог даже предположить, что в скором времени интернет раскроет неограниченные возможности для любого возраста; что свою жизнь можно будет транслировать во всемирную сеть в режиме «онлайн» и эта услуга будет доступна примерно также, как покупка хлеба в ближайшем магазине. Специалистам, которые занимаются вопросами интернет-безопасности нужно ежедневно вместе с подрастающим поколением быть «в тренде» появляющихся социальных сетей, модных приложений, а главное, угроз, которые могут повредить ребенку, в том числе физически.

Возникшие несколько лет назад «синие киты», так взбудоражившие общественность и правоохранительные органы, сегодня, казалось бы, отошли и уже не вызывают опасений. Успокоились напуганные родители, ведь страшное осталось позади, теперь это не модно, а значит можно ослабить бдительность и контроль. Чуть позже, в 2018 году, у детей младшего и среднего школьного возраста возникла новая «забава»: в известном мессенджере WhatsApp стал распространяться модный челлендж «Момо». Это персонаж, один вид которого вызывает ужас и страх, пришел из городской легенды и прочно стал «вирусным в сети». Участникам данного челленджа предлагалось выполнить некоторые задания, связанные с риском для психики и жизни. Аналогичная ситуация была и с сообществами «синих китов».

Такие «киты» и «момо» будут появляться, к сожалению, всегда. Будут разные названия, виды, формы, но будет одна суть – напугать ребенка, подчинить его своим страхам, заставить его сделать что-то противоправное или угрожающее его жизни и здоровью. Часто за всем этим стоит взрослый человек, «куратор», который, возможно не до конца отдает отчет серьезности своих намерений, но тем не менее, совершает страшное преступление. Поэтому сегодня очень важно, чтобы рядом с ребенком был другой взрослый, тот, который не просто проконтролирует, а научит, поможет, защитит. Но помочь ребенку правильному общению в интернете, основам безопасности в сети может только тот взрослый, который умеет это сам. Сегодня, к сожалению, не только родители, но и некоторые педагоги некомпетентны в подобных вопросах, именно поэтому возникает острая необходимость научить каждого человека, как вовремя заметить и предотвратить интернет-зависимость ребенка. Новизна данного мероприятия заключается в описании и мониторинге быстроразвивающихся, возникающих молниеносно социальных сетей.

Целевая аудитория: родители обучающихся, педагоги образовательного учреждения.

Продолжительность занятия по времени: 1 час.

Форма проведения занятия: Проектная задача.

Методы работы: наблюдение, беседа, анкетирование, дискуссия. Индивидуальная и групповая работа.

Глоссарий (основные понятия):

Доступ детей к информации - возможность получения и использования детьми свободно распространяемой информации.

Интернет – всемирная система объединённых компьютерных сетей для хранения, обработки и передачи информации. Упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть.

Кибербезопасность – это защита компьютерных систем, сетей и данных от киберугроз. Для детей – это означает защиту от онлайн-угроз, таких как кибербуллинг, контент несоответствующего содержания и мошенничество.

Кибер-буллинг - вид травли с применением интернет-технологий, включающий оскорбления, угрозы, клевету, компромат и шантаж, с использованием личных сообщений или общественного канала.

Информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Информация, причиняющая вред здоровью и (или) развитию детей, - информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с Федеральным законом РФ от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

Социальная сеть – онлайн-платформа, которую люди используют для общения, создания социальных отношений с другими людьми, которые имеют схожие интересы или офлайн-связи.

Фейковая страница - это аккаунт, созданный от имени другого человека. Подобные страницы делаются с целью продвижения ресурсов, мошенничества или распространения сомнительных файлов.

Место проведения: образовательное учреждение

Материалы (оборудование): мультимедийный проектор, раздаточный материал, ручки.

Цель занятия: повышение уровня компетентности родителей в вопросах обеспечения контроля и безопасности детей в социальных сетях.

Задачи занятия:

1. Систематизирование знаний родителей о влиянии Интернета на детей
2. Ознакомить родителей с рисками и угрозами сети Интернет, в том числе в социальных сетях.

3. Научить родителей основным методам мониторинга детей в социальной сети, оказания им помощи со стороны взрослых.
4. Создание буклета о правилах безопасности детей в сети Интернет.

Ход работы

1. **Предварительный (подготовительный) этап.**

Данный этап реализуется за 5-7 дней до родительского собрания. Участникам обозначается тема и цель мероприятия, родители и обучающиеся на данном этапе будут проанкетированы по вопросам безопасного поведения в сети (**Приложение 1**).

2. **Вступительная часть.**

Добрый день, уважаемые родители. Мы рады приветствовать вас на родительском собрании. Предлагаем вам ознакомиться с правилами и принципами сегодняшнего родительского собрания.

Первый и главный принцип – **принцип равенства.** Все, находящиеся здесь имеют равные права и возможности высказать свое мнение, ничье мнение не будет считаться априори правильным или напротив - неверным, каждый имеет право отстаивать свою субъективную точку зрения. Второй принцип – **принцип взаимного уважения**. Точка зрения вашего оппонента может кардинально отличаться от вашей точки зрения, вследствие чего возникают споры. И хотя говорят, что именно в споре рождается истина, мы должны соблюдать этот принцип – уметь выслушать другую сторону и уважительно отнестись к чужому мнению. Третий принцип - **принцип добровольности**. Участие в нашем мероприятии, конечно добровольное, равно как и желание высказаться, но нам бы хотелось, чтобы родительское собрание прошло в активной, доброжелательной, рабочей атмосфере.

Попробуем вместе с вами определить тему сегодняшнего родительского собрания. Обратите внимание на экран проектора (на экране демонстрируется короткий ролик «Защити ребёнка от интернета». https://youtu.be/8ua0s1bW670?si=SggcRmeiijOQXw5J Данный ролик представляет собой видеоряд подозрительных гостей, которые приходят в гости к ребёнку. В конце ролика задается риторический вопрос: «В реальной жизни вы бы защитили своего ребенка, почему бы не сделать это в интернете?»).

(Родители формулируют тему родительского собрания).

Сегодня такое время, что практически никто из нас не может представить свою жизнь без телефонов, интернета, социальных сетей, даже пожилые люди переписываются с подругами в социальной сети Одноклассники, учреждения ведут деловую переписку в WhatsApp, Телеграмм, ВКонтакте дети снимают путь из школы на видео и одновременно выкладывают это в

интернет. Так ли это опасно, как говорят повсеместно и в СМИ, и на законодательном уровне, и на улице, и в школе; стоит ли бить тревогу и есть ли смысл лишить ребенка полностью доступа в виртуальную сеть, будем разбираться сегодня вместе с вами.

А теперь, давайте сформулируем проблему, с которой сталкиваются родители современного ребёнка. Какая самая большая опасность может поджидать наших детей в Интернете? (Обсуждение проблем).

Исходя из сказанного, предлагаем вам более углубленно изучить данные проблемы.

1. Причины детской зависимости от социальных сетей (приложение 2).
2. Опасности, поджидающие ребёнка в сети интернет (приложение 3).
3. Что делать, что бы оградить ребёнка от негативного воздействия в сети интернет (приложение 4).

3. **Дискуссионный этап** (активизация аудитории).

Для начала нашей работы нам нужно разделиться на три команды. Перед вами лежит информационный материал. Первая группа в течение 10 минут отвечает на вопрос: «Причины детской зависимости от социальных сетей». Вторая группа в течение этого же времени отвечает на вопрос: «Опасности, поджидающие ребёнка в сети интернет» и третья группа в течение этого же времени отвечает на вопрос: «Что делать, что бы оградить ребёнка от негативного воздействия в сети интернет». После того, как пройдет отведенное время, мы выслушаем каждую группу (на данном этапе группы должны активно включиться в работу, в группах должно происходить активное обсуждение – 10 минут).

Итак, время вашего обсуждения подошло к концу и сейчас каждая группа представит ответ на поставленный вопрос. (Выступление групп)

4. **Подведение итогов:**

Сегодня мы проделали большую работу. И дело даже не в том, что мы узнали что-то новое в сложном мире интернета. Самое главное, мы нашли с вами пути решения «Как обезопасить ребенка в современном информационном обществе». Давайте сформулируем правила.

Первое правило, которое родилось в ходе нашей дискуссии: не запрещать, а помогать! Запрет сформулирует у ребенка силу сопротивления и станет невидимой стеной между вами. Он все равно захочет в этот виртуальный мир, но только вы об этом не узнаете**. Второе правило** – разрешай, но проверяй. Контроль его жизни в телефоне должен быть систематический, но очень осторожный, чтобы не потерялось главное между вами – доверие. **Третье правило** – мысли как ребенок! Будьте в курсе всех

новых, модных среди детей социальных сетей и приложений, даже если вам придется устанавливать их на свой телефон и изучать их особенности. И **последнее**, но, пожалуй, самое главное правило – тратьте на своих детей в два раза меньше денег и в два раза больше времени.

4. **Рефлексия (анализ занятия):**

Сегодня для многих из нас открылось что-то новое, наверное, прежде всего в самих себе. Надеемся, что тема нашего родительского собрания не оставила никого равнодушным, ведь у каждого из нас есть ребенок, которого нужно научиться понимать и принимать, которому именно мы, взрослые, обязаны оказать поддержку и помощь. Предоставляем вам буклеты в которых собрана полезная информация «Что делать, что бы оградить ребёнка от негативного воздействия в сети интернет» **(приложения 5)**. Надеемся, что информация в дальнейшем поможет вам немного лучше узнать ребенка и помочь ему правильно использовать интернет.

На доске изображен телефон, на который родители должны прикрепить стикер с ответом на вопрос « Что я сегодня уношу с собой?»

Это то, что вы сегодня нового и полезного уносите с собой и то, что останется с вами навсегда.

На этом наше родительское собрание подошло к концу. До новых встреч.

Список использованной литературы.

1. Чего боятся родители в интернете? **https://www.pravmir.ru/deti-v-internete-4-glavnyih-opasnosti-i-kak-ot-nih-zashhititsya/**
2. Дрепа М.И. Интеренет-зависимость как объект научной рефлексии в современной психологии // Знание. Понимание. Умение. – 2009. - № 2. – Р. 189-193
3.Причины детской зависимости от социальных сетей **https://rskrf.ru/tips/eksperty-obyasnyayut/www-deti/**

Приложение 1.

Анонимное анкетирование родителей
«Знаете ли вы что делают ваши дети в Интернете?»

1. Пользуется ли ваш ребенок интернетом? Если да, как часто?
2. Пользуетесь ли вы сами интернетом?
3. Имеете ли вы доступ к социальным сетям вашего ребенка?
4. Как вы думаете, есть ли у вашего ребенка в сети вторая «фейковая страница»?
5. Делится ли ваш ребенок с вами тем, чем он увлекается в сети?
6. Знаете ли вы основы безопасного поведения в интернете?

Приложение 2

Интернет-зависимость у подростков – это форма аддикции, которая характеризуется чрезмерным увлечением виртуальной средой и стремлением ухода от реальности. Она сопровождается психофизиологическими изменениями поведения, выраженным дискомфортом при невозможности получить доступ к компьютеру и интернету. Такое состояние приводит к социальной дезадаптации, проблемам с успеваемостью, депрессивным расстройствам. Диагностика интернет-аддикции проводится по результатам клинической беседы и специальных опросников. Для лечения используют методы индивидуальной и семейной психотерапии.

Основным фактором развития интернет-зависимости у подростков называют желание сбежать от скуки и проблем реального мира (эскапизм) и найти среду, которая дает ощущение комфорта. Ввиду доступности веб-ресурсов, широкого выбора тематических сообществ в соцсетях, привычки постоянно пользоваться гаджетами интернет становится наиболее подходящим вариантом. Быстрому формированию аддикции способствуют такие факторы:

Потребность в самореализации. В подростковом возрасте обостряется желание самоутвердиться и достичь высокого социального положения. Ребенок использует виртуальную среду, чтобы поделиться истинными или мнимыми достижениями, получить позитивные отклики, ощутить собственную значимость в глазах других людей.

Низкая самооценка. Закомплексованность, чувство неполноценности и неудовлетворенность собой – типичные черты интернет-аддиктов. Обезличенное общение в сети позволяет реализовать любые фантазии и представить себя совершенно другим человеком, на которого подростку хотелось бы быть похожим.

Отсутствие друзей. Многие интернет-зависимые подростки испытывают трудности в реальном общении, вызванные комплексами и другими факторами. В сети они могут получить безопасное и разнообразное общение, без стеснения знакомятся с большим количеством новых людей, что создает иллюзию насыщенной социальной жизни.

Семейные проблемы. Подростки используют сетевые игры и общение в соцсетях как способ снять тревожность и эмоциональное напряжение, найти «понимающих» собеседников. Тяга к интернет-аддикции встречается как в семьях с высоким социальным статусом, где у взрослых нет времени

заниматься воспитанием детей, так и в неблагополучных и асоциальных семьях.

Поведение родителей. Привычка с раннего возраста давать ребенку смартфон или планшет, чтобы его быстро успокоить и чем-нибудь занять в очереди или в поездке, имеет негативные последствия в более старшем возрасте. Так формируется привычка использовать гаджет для эмоциональной разгрузки, максимально проявляющаяся в подростковом периоде.

Одним из пусковых факторов интернет-зависимости у подростков называют популяризацию IT-профессий. Программирование, веб-дизайн, цифровой маркетинг – востребованные направления, где люди могут реализовать себя и уже в молодом возрасте достичь значительных успехов, в том числе финансовых. При наличии акцентуаций личности и проблем с социализацией изначально положительное стремление к знаниям трансформируется в аддикцию.

Патология относится к нехимическим аддикциям. Систематизация интернет-зависимости представляет сложности для практической психиатрии, поскольку в международных системах DSM-V и МКБ-10 такой диагноз не представлен. Наибольшую популярность получила классификация по K. Young, согласно которой существует 5 клинических форм болезни:

Компьютерная зависимость. Наиболее популярная форма интернет-зависимости у подростков, которая проявляется навязчивым желанием играть в компьютерные игры.

Киберсексуальная форма аддикции. Увлечение просмотром порнографических материалов, участие в приватных беседах «для взрослых», которые могут сопровождаться обменом интимными фотографиями, демонстрацией сексуальных девиаций.

Киберотношения. Постоянное общение в мессенджерах и социальных сетях, активное участие в сообществах по интересам, если при этом подросток игнорирует взаимодействие с реальными друзьями и членами семьи.

Информационная перегрузка. Регулярное использование новостных веб-ресурсов и информационных сайтов для получения новых данных. Состояние сопровождается ощущением «упущенных возможностей», если подросток лишен возможности воспользоваться интернетом.

Сетевая вовлеченность. Участие в сетевых азартных играх и аукционах, желание постоянно совершать покупки в онлайн-магазинах, многочасовой выбор и складывание «в корзину» товаров, которые подросток даже не собирается покупать.

Интернет-зависимость у подростков

Симптомы

Интернет-зависимость у подростков сопровождается утратой критики к своему состоянию, поэтому первые признаки проблемы замечают окружающие: родители, одноклассники, школьные учителя. Подросток с интернет-зависимостью начинает все больше времени проводить за использованием телефона, планшета или компьютера, игнорируя реальную жизнь. Увлечение виртуальным миром происходит в ущерб учебе, активному отдыху, общению со сверстниками.

Подростки начинают обманывать родителей и скрывать, какое количество времени проводят в сети. Многие тайком сидят в интернете всю ночь, прогуливают школу, кружки и занятия с репетитором, чтобы больше времени потратить на сетевые развлечения. Это сопровождается изменением привычек и образа жизни: ребенок становится неряшливым, пропускает приемы пищи, забывает о просьбах родителей и систематически не делает домашние задания.

Для интернет-зависимости у подростков характерен «синдром отказа», который возникает спустя несколько дней вынужденного ограничения

использования гаджетов. Он проявляется повышенной тревожностью, раздражительностью, психомоторным возбуждением. Пациента постоянное беспокоят навязчивые мысли о происходящем в интернете, появляется чувство, что он пропускает что-то важное (синдром упущенной выгоды – FOMO).

Интернет-аддикция сопровождается легкими признаками физической зависимости. Многие пациенты страдают от нарушений сна и навязчивых сновидений в виде пассивного «просмотра текста». Нарушения работы вегетативной нервной системы проявляются патологиями сердечного ритма, склонностью к гипо- или гипертензии, повышенной потливостью. Недомогание усиливается, если подросток длительное время лишен возможности выйти в сеть.

Осложнения

Хотя интернет-зависимость считается менее опасной, по сравнению с химическими аддикциями, она чревата серьезными проблемами. Последствия зависят от того, как именно подросток проводит время в интернете. Наиболее опасны «группы смерти» – сообщества в соцсетях, где участники получают различные задания, финальной целью которых выступает суицид. В России ежегодно совершается несколько сотен детских самоубийств, многие из которых имеют связь с подобными группами.

Большое опасение вызывает создание и эксплуатация виртуального образа «Я», которое сильно отличается от реальной личности подростка. Постепенно такой разрыв усугубляется, ребенок чувствует себя комфортно только в выдуманном мире интернет-собеседников и компьютерных игр. Это приводит к социальной нереализованности, тревожно-депрессивным расстройствам, проблемам в построении романтических отношений в будущем.

Интернет-зависимость у подростков осложняется физическими симптомами. Постоянное использование гаджетов вызывает давящие головные боли, которые по интенсивности и характеру напоминают мигрень. Однообразная постановка рук для удержания мышки и набора текста на клавиатуре/экране смартфона вызывает синдром карпального канала. Многие дети сталкиваются с быстрым ухудшением зрения, синдромом «сухого глаза». Сидение в неудобной позе провоцирует боли в спине и шее.

Диагностика

Если родители замечают у подростка чрезмерную увлеченность интернетом, нужно обратиться к детскому психологу. Беседа проводится с ребенком и членами семьи, поскольку аддикты не могут корректно оценить свое состояние и время, проведенное в сети. Большинство подростков категорически опровергают наличие зависимости и с трудом идут на контакт, поэтому от врача требуется терпение и профессионализм. Чтобы определить факт интернет-аддикции, используются:

Клинические критерии. Основой для диагностики зависимости служат 2 фактора: толерантность – необходимость постоянно увеличивать время, проведенное в интернете, и «синдром отмены» – негативные психологические реакции на лишение доступа к сети. Аддикция более вероятна, если такие признаки сопровождаются проблемами в личной и социальной сфере, связанными со злоупотреблением гаджетами.

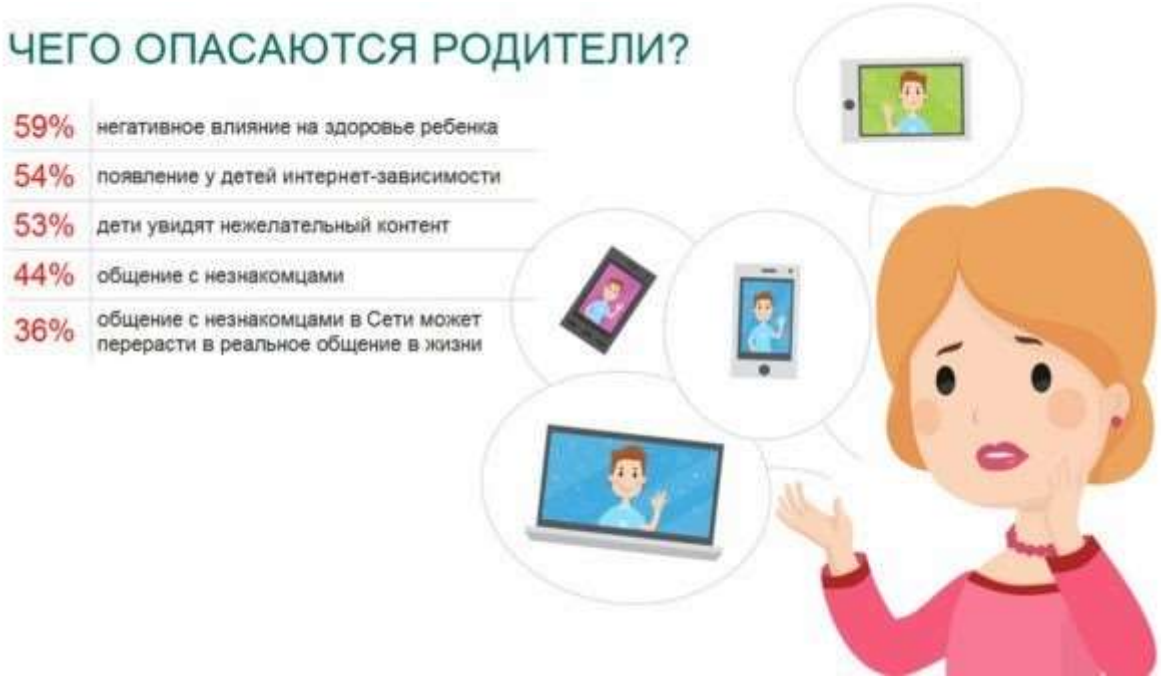
Тесты и опросники. Самая известная методика – тест Кимберли Янга, который в российской врачебной практике применяется в адаптации В. Лоскутовой. В медицинской психологии также широко используют шкалу интернет-зависимости Чена (CIAS), диагностический опросник интернет-аддикций, восьмипунктовый опросник Сэлливана и Канадский подростковый опросник.

Прогноз и профилактика

Интернет-зависимость не вызывает необратимых изменений в психических процессах и успешно поддается коррекции объединенными усилиями психологов, родителей и самого подростка. Однако тяга к эскапизму и аддиктивному поведению может стать причиной повторения симптомов, возникновения разных видов нехимической (гэмблинг, любовная зависимость) или химической зависимости (алкоголизм, токсикомания, наркомания).

Для профилактики интернет-аддикции родителям нужно обращать внимание, сколько часов подросток проводит за компьютером, интересоваться его виртуальными друзьями и сайтами, которые он регулярно посещает. Нужно постараться, чтобы реальная жизнь ребенка была интересной и отвечала его представлениям: организовать посещение спортивной секции, занятий музыкой и других кружков по интересам, в пределах разумного позволять прогулки и посиделки со сверстниками.

Приложение 3



Утрата денег

Первый вид опасностей – те, которые связаны с кражей денег.

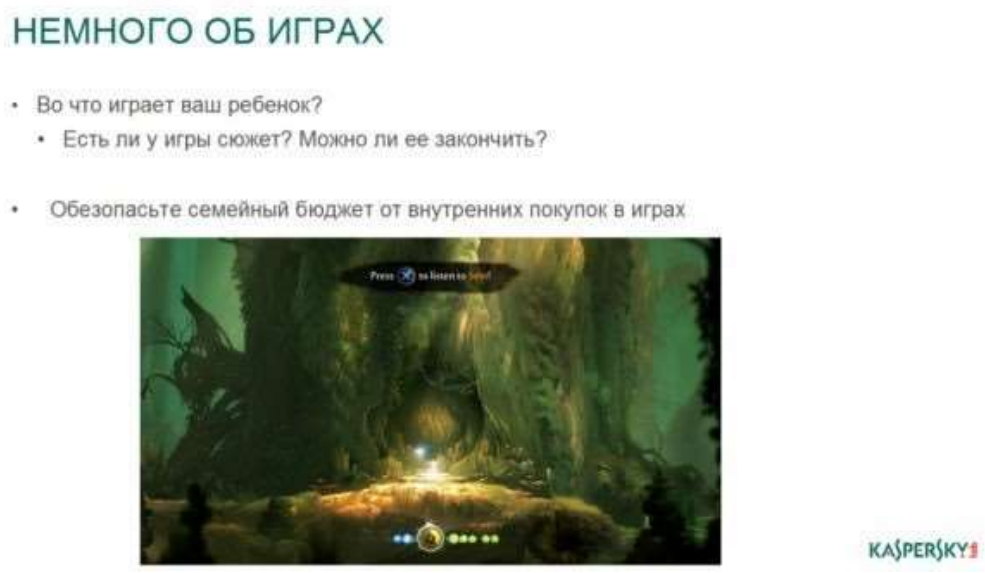
Фишинг – это выманивание паролей от различных сервисов, в том числе личных страниц во «ВКонтакте» или Steam, чем дети-подростки обычно очень дорожат. Их крадут, чтобы получить доступ к персональной информации, чтобы делать спам-рассылки, чтобы продолжать использовать – например, аккаунты игровой платформы Steam, где распространяются игры и есть своя социальная сеть.

Steam – это рекордсмен по числу онлайн-пользователей, их там больше, чем даже в YouTube. Поскольку участники покупают игры на свой аккаунт, «развивают» своих персонажей в многопользовательских онлайн-играх, «заливают» туда деньги и время, эти аккаунты могут достаточно дорого стоить – страничка с 1000 наигранных часов в какую-нибудь популярную многопользовательскую игру с очень развитым персонажем продастся на черном рынке за весьма неплохие деньги.

Еще одна техническая опасность – **вредоносный код**: например, пользователь перешел по какой-то ссылке, и компьютер заблокировался, и теперь пользователь видит только сообщение «Заплатите деньги туда-то, и компьютер разблокируется». Причем гарантии, что он разблокируется после оплаты, к сожалению, нет. Есть и другой вредоносный код: тот, что незаметно работает на компьютере, отправляя злоумышленникам те же логины/пароли или данные платежных карт.

Обычное мошенничество – в интернете встречается так же часто, как и в реальной жизни. Его можно охарактеризовать всем известной поговоркой «Бесплатный сыр бывает только в мышеловке». Например, предлагается купить смартфон по цене значительно ниже рыночной, человек отправляет деньги, но телефон так и не получает. Это очень популярная схема мошенничества: дорогой товар за небольшие деньги. И это очень хорошо срабатывает в ситуации с подростками, потому что они часто прицельно копят деньги на какой-нибудь игровой компьютер, и если они внезапно видят его не за 60, а за 20 тысяч рублей, то могут с радостью заказать его и перевести деньги.

Определенную опасность для семейного бюджета представляют также и онлайн-игры – в них часто есть **встроенные внутренние покупки**. Чтобы обезопасить себя от этих трат, убедитесь, что ребенок не может тратить деньги с вашей карточки, привязанной к онлайн-игре, в том числе и если он зайдет в вашу игру.



Это может происходить, если система запрашивает подтверждение не каждый раз при совершении покупки, а, например, раз в полчаса, раз в сутки. За полчаса можно многое успеть. Одна английская девочка четырех лет, играя, пока папа варил макароны, потратила больше 1000 фунтов, причем ругать ее было за это бесполезно: она просто играла и даже не знала, что тратит деньги, нажимая на «да» и «купить».

Зависимость

Интернет-зависимость чаще всего ассоциируется с играми, и родители, когда говорят о зависимости, имеют в виду прежде всего именно ее.

Сегодня играют все дети, но в разные игры. Глобально их можно разделить на две группы: первая – это **просто игры**, в которые играют час-другой в день, проходят за несколько недель, и все.

Вторая – это так называемые **массовые мультиплеерные онлайн-игры**, в которые можно играть годами, развивая своих персонажей, приобретая для них какие-то качества или оборудование и так далее.

Если ребенок играет в такую игру, надо серьезно подумать, как это ограничивать, потому что такие игры действительно вызывают привыкание как у детей, так и у взрослых.

Происходит это за счет того, что такие игры вбрасывают в детей якоря: один якорь – это социальные связи с другими игроками, которыми ребенок обрастает за время игры, второй – это финансовые вложения: я купил крутой танк, надо на нем покататься, я уже столько сюда вложил, что жалко бросать, третий – это потраченное время: как отказаться от игры, если я играю в нее уже полтора-два года.

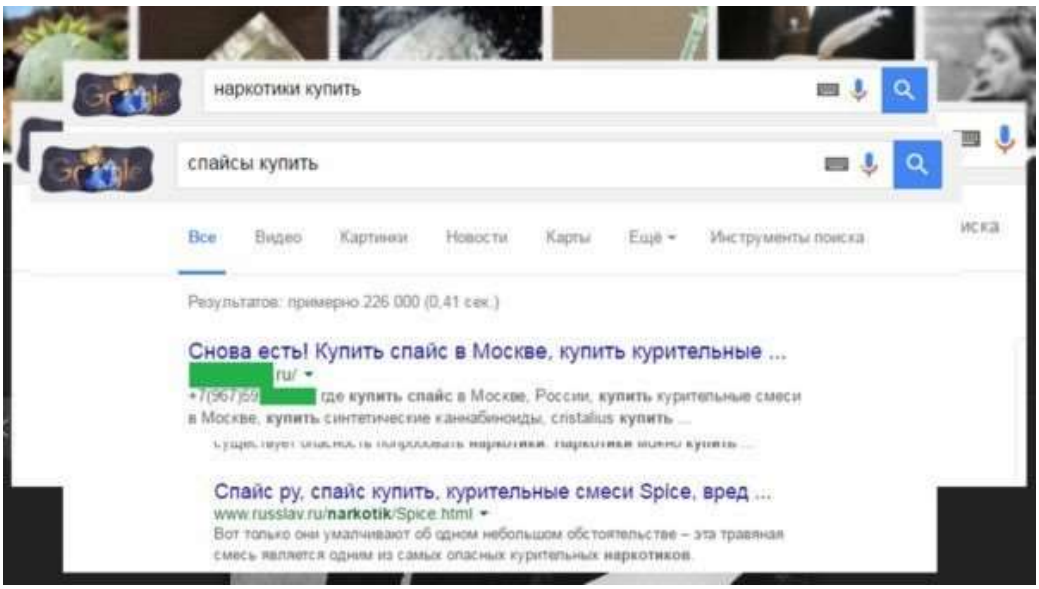
Зависимость – это болезнь, к ней следует так и относиться, и если ребенок ради игры начинает отказываться от еды, от сна, и тем более если проявляет агрессию, когда ему не дают играть, то надо идти к специалисту.

Нежелательное содержание

Помимо порнографии, которая безусловно лидирует в списке того, что родители не хотели бы, чтобы видели их дети, в незащищенном интернете можно увидеть массу других нежелательных вещей. На сайтах новостей достаточно часто появляются фотографии и видеозаписи с мест катастроф, где можно видеть сцены убийства, насилия, аварии, теракты и их последствия. Более того, такие иллюстрации могут оказаться в самых неожиданных местах – например, на безобидном на вид сайте-агрегаторе смешных (!) картинок.

При попытке поиска наркотиков через поисковые системы можно обнаружить на первой же странице результатов не рассказ о последствиях их приема, а контакты продавцов, причем, возможно, сами сайты заблокированы Роскомнадзором и зайти на них нельзя, но контакты могут быть видны на странице поисковых результатов.

И, к сожалению, такие сайты появляются быстрее, чем Роскомнадзор успевает их блокировать. Кроме того, это может быть объявление на сайте, который блокировке не подлежит, – например, в форуме реабилитирующихся. Конечно, через пару часов модераторы его удалят, но какое-то время оно повисит.



Помимо этого, безусловно нежелательным для ребенка контентом является все, что относится к самоубийствам и способам их осуществления, а родителям девочек следует обратить особое внимание на интерес дочерей к картинкам с анорексичными моделями – часто они распространяются как образец для подражания, и из-за этой пропаганды, особенно если она исходит от подруг, девочки начинают терзать себя диетами и отказываются от еды.

Незнакомцы

На занятиях я объясняю подросткам – а они этому обычно очень удивляются, – что у взрослых, как правило, нет первоочередной цели пообщаться, в отличие от подростков, которые идут в интернет в основном за этим.

У нормального взрослого человека нет безудержного желания общаться с незнакомыми детьми, добавлять их в друзья, начинать с ними интенсивную коммуникацию, и, как правило, если взрослый человек приходит к незнакомому подростку, значит, ему наверняка что-то от него нужно.

По нашим исследованиям, 90% московских школьников получают в интернете предложение о дружбе от незнакомых людей, и 53% их принимают. Разговаривая об этом с детьми, я привожу такой пример: к тебе на улице подходит молодой человек лет тридцати пяти, называет тебя по имени и говорит: «Аня, давай дружить!» Большинство, конечно, отвечают, что они убегут. Однако когда то же самое происходит в сети, они совершенно спокойно начинают с этим человеком общаться.

Проблема состоит в том, что многие подростки чрезвычайно доверчивы, и незнакомец, который с какой-то целью хочет «подружиться» с ребенком, может за считанные недели в его глазах стать самым близким его человеком, единственным, кто его понимает и так далее. Достигается это с помощью манипулятивных техник и самых простых приемов, вплоть до активного

слушания, когда ребенок что-то рассказывает собеседнику, собеседник повторяет это своими словами, и ребенок думает: о, он меня понимает, как никто! (Кстати, попытка втереться в доверие ребенка с тем, чтобы в дальнейшем его как-то использовать, называется **онлайн-грумминг**.)

Ребенок начинает относиться к этому человеку как к действительно близкому и заслуживающему того, чтобы с ним делились и самой интимной информацией, и контактными данными, и фотографиями, не предназначенными для чужих глаз.

Если хотите, проведите эксперимент: возьмите в интернете фото какого-нибудь юного мулата, назовите его, например, Хорхе Домингос, сделайте аккаунт во «ВКонтакте», напишите, что ему 15 лет и попробуйте добавиться в друзья к подросткам. Вы увидите, как они легко и быстро внесут вашего Хорхе в свой список друзей – никому из них не придет в голову проверить имя, фамилию и фотографию, а если вдруг и придет, то вы можете вздохнуть и сказать: да, это правда, я не Хорхе, я на самом деле Ваня Иванов, вот мое фото – и пошлете другую чужую фотографию, и тогда они уж точно будут уверены в том, что вы написали правду.

Я в принципе против общения с незнакомыми людьми в интернете – именно потому, что нет никакого способа убедиться в том, что этот человек – тот, за кого он себя выдает, и если из ста случаев всего один – это человек с преступными намерениями, все равно это повод, чтобы никому не доверять. Вы просите фото, чтобы удостовериться в том, что пол и возраст соответствуют заявленным – и получаете того же условного Хорхе Домингоса.

Разговор по скайпу дает большую уверенность, но если это, например, группа педофилов, у них может быть «на крючке» ребенок, которого они с этой целью используют. Конечно, это достаточно сложная конструкция, но некоторая вероятность такого варианта есть, а значит, этот вариант тоже не дает стопроцентной уверенности.

Самый надежный способ убедиться в том, что человек – тот, за кого он себя выдает, и это же самый опасный способ – личная встреча. Если ребенок пришел на встречу, и там оказался его ровесник, и они два часа прообщались, и его не завербовали в секту, не продали ему наркотики и не посадили в машину к взрослому дядьке, который не увез его в лес и не оставил там убитым, то на следующей встрече вряд ли произойдет что-то из перечисленного, но, конечно, проверять таким способом, случится ли все это, нельзя.

Кстати, несмотря на то, что большинство родителей думает: ладно, пусть общается с кем угодно в интернете, он же умный и на личную встречу не пойдет, 55% детей по нашим опросам положительно отвечают на вопрос «Принимаете ли вы приглашения дружить от незнакомых людей» и 45% из них готовы встречаться лично, а многие пишут в анкете: «А я уже встречался!»

Более или менее безопасная встреча – это когда встречаются целой группой с форума по интересам или из игры – например, командой игроков в танки (пять человек) или даже целой гильдией (тридцать, пятьдесят человек). Встретились, посмотрели друг на друга, убедились, что это реальные люди, соответствующие заявленному возрасту и полу. Если мы говорим об играх, то убедиться в том, что товарищи по игре – те, за кого они себя выдают, позволяет TeamSpeak: система коллективного общения через гарнитуру во время игры. Так слышно, по крайней мере, мужчина там или женщина, взрослый или ребенок.

Проверка IP-адреса, геопривязки фотографий и прочего – это занятие для профессионалов из, скажем, МВД или ФСБ, в домашних условиях получить достоверную информацию в результате такого «расследования» сложно.

Безусловно, незнакомец может действительно оказаться ровесником ребенка, который просто хочет общаться по причине сходства интересов, потому что понравилась фотография и т.д., но, поскольку достоверно установить это нельзя, ребенок должен понимать, что там, где размещается его персональная информация, он должен к каждому относиться с недоверием.

Периодически разработчики предлагают технологии, позволяющие устанавливать личность каждого человека, входящего в интернет, но мы же все против. Идея того же входа во «ВКонтакт» по паспортам была отвергнута, потому что мы за тайну частной жизни и приватное общение. Безопасность и приватное общение всегда на весах друг против друга, и сегодня общество выбирает приватность.

Конечно, никто никого не убивал, но это были очень эффективные «страшилки» за счет того, что в них было очень много персональных данных.

Приложение 3

Как защитить ребенка от негативного воздействия интернета.

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

1. Прежде, чем позволить ребенку пользоваться Интернетом, расскажите ему о возможных опасностях Сети (вредоносные программы, небезопасные сайты, интернет-мошенники и др.) и их последствиях.
2. Четко определите время, которое Ваш ребенок может проводить в Интернете, и сайты, которые он может посещать.
3. Убедитесь, что на компьютерах установлены и правильно настроены антивирусные программы, средства фильтрации контента и нежелательных сообщений.
4. Контролируйте деятельность ребенка в Интернете с помощью специального программного обеспечения.
5. Спрашивайте ребенка о том, что он видел и делал в Интернтете
6. 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.

7. 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.
8. 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.
9. Объясните ребенку, что нельзя открывать файлы, полученные от неизвестных пользователей, так как они могут содержать вирусы или фото/видео с негативным содержанием.
10. Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации.
11. Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека.
12. Постараться регулярно проверять список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются;
13. 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;
14. Проверяйте актуальность уже установленных правил. Следите за тем, чтобы Ваши правила соответствовали возрасту и развитию Вашего ребенка.

Как помочь

Что делать, если ребенок уже столкнулся с какой-либо интернет-угрозой

1. Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать.
2. Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или он попал в неприятную ситуацию (потратил деньги в результате интернет-мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации. Выясните, что привело к данному результату – непосредственно действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в интернете.
3. Если ситуация связана с насилием в интернете в отношении ребенка, то необходимо узнать информацию об обидчике, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно обидчику о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. п.). Объясните и обсудите, какой опасности может подвергнуться ребенок при встрече с незнакомцами, особенно без свидетелей.
4. Соберите наиболее полную информацию о происшествии – как со слов ребенка, так и с помощью технических средств. Зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.

5. В случае, если вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, или ребенок недостаточно откровенен с вами и не готов идти на контакт, обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации и подскажут, куда и в какой форме обратиться по данной проблеме.

Предупреждение столкновения с вредоносными программами

1. Установите на все домашние компьютеры антивирусные программы и специальные почтовые фильтры для предотвращения заражения компьютера и потери ваших данных. Подобные программы наблюдают за трафиком и могут остановить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
2. Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.
3. Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.
4. Следите за тем, чтобы ваш антивирус регулярно обновлялся, и раз в неделю проверяйте компьютер на вирусы.
5. Регулярно делайте резервную копию важных данных, а также научите это делать ваших детей.
6. Старайтесь периодически менять пароли (например, от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т.п).
7. Расскажите ребенку, что нельзя рассказывать никакие пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.
8. Расскажите ребенку, что если он пользуется интернетом с помощью чужого устройства, он должен не забывать выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы. Никогда не следует сохранять на чужом компьютере свои пароли, личные файлы, историю переписки — по этой информации злоумышленники могут многое узнать о вашем ребенке.

Как избавиться от вредоносных программ

1. Загрузите компьютер в безопасном режиме (включите компьютер, нажмите и, удерживая клавишу F8, выберите Безопасный режим (Safe Mode) в открывшемся меню).
2. Проведите полную антивирусную проверку компьютера.
3. Если в результате проверки обнаружен вирус, червь или троянская программа, следуйте указаниям производителя антивирусного ПО. Хорошие антивирусы предлагают лечение зараженных объектов, помещение подозрительных объектов в карантин и удаление троянских программ и червей.
4. При невозможности самостоятельно решить проблему обратитесь за помощью в службу технической поддержки производителя

установленного на вашем компьютере антивирусного ПО или в технический сервис.

Беседа для родителей «Как защитить ребенка от негативного влияния интернета?»

1. **Интересуйтесь жизнью ребенка.**

Как можно чаще разговаривайте с **ребенком** (о его и ваших радостях, огорчениях, открытиях, планах, мечтах, **интересах**). Старайтесь понять мысли и чувства **ребенка.**

Приглашайте в гости его друзей. Знайте, в каком окружении он вращается, чем занимается, с кем дружит, чем они увлекаются, к каким молодежным субкультурам приобщаются. Ведь дети выбирают не наркотики, они выбирают сначала стиль жизни, и если этот стиль предполагает употребление наркотиков, то они приобщаются и к употреблению.

Если ваш **ребенок** уже в подростковом возрасте – добавьте его в друзья в социальных сетях. Вы сразу увидите, чем **ребенок интересуется**, какие проблемы его волнуют. Достаточно посмотреть, что он постит, какими ссылками обменивается, какую музыку скачивает, какие фильмы смотрит, в каких группах состоит, с кем дружит. Но при этом важно соблюдать деликатность. Это не должно быть способом вынюхивания компромата, чтобы потом спустить на **ребенка всех собак**. Так вы можете потерять его доверие.

В этом возрасте у подростка очень хрупкое *«Я»*, неустойчивая система личности. А чувства переживаются очень сильные и яркие. Обсуждая какое-нибудь событие из его жизни, ни в коем случае нельзя пренебрежительно говорить *«Мне бы твои проблемы!»* или *«Ерунда, скоро всё пройдет!»*. Лучше расскажите о своем пережитом опыте (первой любви, первом экзамене, первой победе, первом пережитом вами предательстве и пр.).

2. Договоритесь о правилах пользования **Интернетом.**

Для лучшего взаимопонимания и устранения возможных недоразумений, лучше сразу расставить все точки над *«i»*, установить некоторые ограничения для самостоятельного выхода в **Интернет**. Составьте список правил работы детей в **Интернете и помните**, что лучше твердое *«нет»*, чем неуверенное *«да»*. Пусть ограничения будут минимальны, но зато действуют всегда.

Оговорите, сколько времени он может проводить в **Интернете.**

Объясните **ребенку**, что недопустимо выкладывать в сеть личные данные *(Ф. И. О., возраст, город, место учебы, домашний адрес, номер телефона)* и конфиденциальную информацию (время возвращения из школы, место прогулок, компрометирующие фотографии).

3. Используйте возможности **интернета с пользой.**

Помогите **ребенку** найти чаты и форумы по его **интересам**, направьте его в нужное русло, и он будет меньшее время проводить в поиске какой-либо информации, дрейфуя по сайтам и натыкаясь на ссылки с сомнительными ресурсами.

В этих же целях для маленького **ребенка** установите на компьютер детскую поисковую систему. Помните, что вы можете, не читая переписки,

отслеживать время от времени посещаемые **ребенком** сайты по ссылкам в журнале истории браузера.

4. Не теряйте бдительности.

Время от времени посещайте любимые сайты **ребенка вместе с ним.** Если **ребенок ведет дневник в Интернете**, иногда прочитывайте его.

Чаще разговаривайте с **ребенком** об обсуждаемых в чате темах, **собеседниках**, что его **заинтересовало или насторожило.**

Регулярно проверяйте содержимое памяти компьютера *(не сохранены ли в ней сомнительные материалы)***.**

Помните!

1. Будьте в курсе того, чем занимаются ваши дети в **Интернете.** Попросите их научить вас пользоваться различными приложениями, которыми вы не пользовались ранее.

2. Помогите своим детям понять, что они не должны размещать в Сети информацию о себе: номер мобильного телефона, домашний адрес, а также показывать фотографии *(свои и семьи)*. Ведь любой человек может это увидеть и использовать в своих **интересах.**

3. Если ваш **ребенок получает спам** (нежелательную электронную почту, напомните ему, чтобы он не верил написанному в таких письмах и ни в коем случае не отвечал на них.

4. Объясните детям, что нельзя открывать файлы, присланные незнакомыми людьми. Эти файлы могут содержать вирусы или фото-, видеоматериалы непристойного или агрессивного содержания.

5. Объясните, что некоторые люди в **Интернете** могут говорить неправду и быть не теми, за кого себя выдают. Дети никогда не должны самостоятельно, без взрослых встречаться с сетевыми друзьями, которых не знают в реальной жизни.

6. Постоянно общайтесь со своими детьми, рассказывайте, советуйте, как правильно поступать и реагировать на действия других людей в **Интернете.**

7. Научите своих детей правильно реагировать, если их кто-то обидел в Сети или они получили / натолкнулись на агрессивный контент. Расскажите, куда в подобном случае они могут обратиться.

8. Убедитесь, что на компьютере, которым пользуются ваши дети, установлены и правильно настроены средства фильтрации.

Наши дети-наше будущее!

Безопасность в интернете: возрастные рекомендации для детей и подростков

Дети и подростки используют интернет по-разному и для разных целей по мере взросления. Родители детей из каждой возрастной группы беспокоятся о разных вещах и хотят контролировать разные действия. Однако есть набор общих рекомендаций, которые следует помнить родителям детей и подростков любого возраста.

Храните имена пользователей и пароли в безопасности

Для многих используемых детьми веб-сайтов требуется имя пользователя и пароль. Убедитесь, что дети знают, что эту информацию нельзя передавать никому, даже друзьям. Возможно, никто не хочет причинить ребенку никакого вреда, но даже в розыгрышах из лучших побуждений что-то может пойти не так и доставить неприятности. Храните имена пользователей и пароли в секрете и обязательно меняйте пароли, если подозреваете, что кто-то мог их узнать.

Периодически меняйте пароли

Наряду с напоминанием детям о том, что никому нельзя сообщать свои пароли, также рекомендуется периодически менять пароли. Утечки данных происходят постоянно, а утечка паролей подвергает риску кражи личных данных и другим проблемам с кибербезопасностью. Настройте расписание смены паролей учетных записей каждые 3-6 месяцев или каждый раз, когда платформа сообщает о взломах или утечках данных. Вы можете использовать менеджер паролей, чтобы отслеживать все свои пароли в интернете и упростить их поиск вашим детям.

Не разглашайте личную информацию в интернете

Дети и подростки не должны сообщать никому в интернете свое полное настоящее имя, адрес, район проживания, номер телефона и прочие данные. Общее правило: никогда не сообщать информацию, которая могла бы помочь интернет-хищникам найти их. Даже небольших деталей, таких как название школы или спортивной команды, достаточно, чтобы раскрыть личность. Если дети используют сайты, позволяющие общаться с незнакомцами, например, платформы социальных сетей, убедитесь, что они знают, что эта информация является конфиденциальной.

Будьте внимательны в социальных сетях
Действия детей и подростков в социальных сетях требуют особой осторожности и внимания. Интернет огромен, но компрометирующие фотографии, грубые комментарии и личная информация могут оставить сильный след, и часто навсегда. Напомните детям, что все опубликованное в интернете сразу становится общедоступным, и любой может увидеть это. Даже частные учетные записи иногда подвергаются утечкам или атакам злоумышленников. Если вы не хотите, чтобы какой-либо неприятный момент повторялся и тревожил ваших детей, объясните им, что нужно внимательно относиться своим публикациям.

Используйте надежное решение для кибербезопасности

Kaspersky Safe Kids помогает защитить детей, когда они находятся в сети. Это решение можно использовать на всех устройствах вашего ребенка. Оно состоит из двух приложений: одно нужно установить на устройство ребенка, второе – на смартфон родителя, чтобы просматривать отчеты и менять настройки. Встроенный родительский контроль даже позволяет управлять временем, которое дети проводят перед экраном на разных устройствах.

Проверяйте возрастные ограничения

Многие приложения и веб-сайты имеют собственные возрастные ограничения для создания учетных записей, просмотра и регистрации. Но проблема в том, что на большинстве таких сайтов фактически нет функции проверки возраста. Например, Facebook, Snapchat и Myspace разрешают доступ только с 13 лет, но дети могут указать другой возраст и зарегистрироваться в любом случае.

Объясните опасность передачи геоданных

Почти все современные приложения и веб-сайты имеют функции отметки геопозиции или передачи данных о местоположении. Дети и подростки должны знать, чем опасно сообщать о своем местоположении, и что не следует неосознанно соглашаться с таким условием во всплывающих окнах приложений. Публичная демонстрация данных о местоположении подвергает детей различным опасностям: от сетевых интернет-хищников, которые могут найти их, до риска кражи личных данных. Убедитесь, что дети понимают, что означает, когда в приложении спрашивается, можно ли передавать данные о местоположении.

Создайте список правил использования интернета

Один из лучших способов управлять использованием интернета детьми всех возрастов – это сесть и совместно составить список правил использования интернета в соответствии с их потребностями. Вы можете показать ребенку сайты для детей и подростков, поговорить о том, почему важно установить правила, и попросить их поделиться, если он чувствуют себя некомфортно или ему угрожает что-то, найденное в интернете, и т. д. Установите границы, но будьте реалистом.

Используйте одинаковые правила при общении онлайн и лично
Научите детей тому, что к онлайн и к личному общению применимы

одни и те же правила. При общении в интернете и написании комментариев лучше оставаться добрым и вежливым, не следует писать ничего такого, что не смогли бы сказать в лицо. Это также применимо и при анонимной публикации сообщений. Публикация обидных и грубых вещей – это не только некрасиво и нелицеприятно по отношению к другим, но также может навредить репутации вашего ребенка.

Установите родительский контроль

Настройте и пересмотрите параметры родительского контроля на всех своих устройствах в соответствии с возрастом ваших детей. Это поможет защитить детей от доступа к неприемлемому контенту в интернете. Параметры контроля можно настроить несколькими способами, например, обеспечить доступ детей только к соответствующему их возрасту контенту, установить время использования устройства, контролировать активность и запретить передачу личной информации. В дополнение к родительскому контролю можно также использовать инструменты фильтрации и мониторинга. Периодически проверяйте и обновляйте эти программы. Здесь приведена информация о потенциально опасных для детей приложениях и веб-сайтах.

Используйте антивирусные программы.

Помимо родительского контроля, используйте на всех устройствах антивирусные программы. Они защищают подключенные к интернету устройства от входящих угроз, а также выявляют, уничтожают и предупреждают о возможных угрозах для системы. Антивирусные программы не отстают от современных угроз и помогают обнаруживать новые постоянно появляющиеся вирусы.

Расскажите о существовании фальшивых рекламных объявлений

Обсудите с детьми рекламные программы и мошенничество, связанное с фальшивыми рекламными объявлениями, с которыми они могут столкнуться в интернете. Некоторые объявления выглядят как реальные предложения, побуждающие загрузить фальшивое приложение, зарегистрироваться для участия в розыгрыше или предоставить личную информацию в обмен на бесплатные продукты. Они также могут быть представлены в виде ссылок, которыми можно поделиться с друзьями или опубликовать в социальных сетях. Если дети знают о существовании таких видов рекламы и мошенничества, они с меньшей вероятностью попадутся на них, столкнувшись в Интернете.

Объясните детям об опасности личных встреч с незнакомцами

Дети никогда не должны лично встречаться с незнакомцами, с которыми они общались в интернете, если за такой встречей не наблюдает родитель. Объясните детям и подросткам, что не следует общаться с незнакомцами лично. Интернет-хищники или участники кибербуллинга (травли) могут скрываться, чтобы ребенок не понял, что общается с кем-то из интернета.

Мониторинг истории поиска в интернете

Родителям детей любого возраста рекомендуется периодически проверять историю браузера, чтобы понять, какие сайты посещают их дети. Убедитесь, что в настройках браузера включено отслеживание истории, и проверяйте ее

на всех устройствах с доступом в интернет. Если вы столкнетесь с подозрительными сайтами, спросите о них у ребенка. Продемонстрируйте детям максимальную открытость при отслеживании их действий в интернете, чтобы они не ощущали, что за ними шпионят.

Безопасность в интернете: лайфхаки для детей и родителей безопасность детей в интернете

Кибербуллинг, секстинг, кибермошенничество, кража паролей и случайная трата денег... Современные дети ориентируются в интернете и соцсетях лучше, чем их родители. Но неопытных пользователей поджидают опасности и злоумышленники. Как уберечь детей от рисков в Сети?

Тактика родительского контроля меняется каждый год вместе с технологиями. Мы собрали советы для родителей: чему и в каком возрасте научить ребёнка, чего стоит особенно опасаться и какие программы можно использовать для защиты.

Поскольку подростки больше времени, чем взрослые, проводят в инете, они становятся первыми исследователями, первыми сталкиваются с изменениями в сети, а потому и принимают на себя первый удар. Это касается технологических проблем, прежде всего вредоносных программ. Затем идут контентные риски, такие как изображения сексульного характера, содержащие насилие и жестокость. Дальше – коммуникационные риски: травля ребенка и проявление агрессии в сети, пропаганда суицида, анорексии и булимии. В последнее время очень опасным явлением в интернете стала вероятность столкновения детей в сети с агрессией (кибербуллингом) и сообщениями сексуального характера (секстинг, груминг).

”Уже разработаны рекомендации для родителей, как защитить ребенка от нежелательного контента в интернете, как научить его быть осторожным при знакомстве и общении он-лайн, как избежать интернет-мошенничества. Однако нужно помнить, что никакие технологии, даже самые инновационные, не заменят родительского контроля. Поэтому, даже если вы установите все рекомендуемые настройки, главная задача – лично рассказать ребенку о правилах безопасности в сети.

Советы взрослым: как обезопасить детей в интернете

Используйте программное обеспечение, помогающее фильтровать и контролировать информацию (например, AiProtection в Wi-Fi-маршрутизаторах ASUS, менеджер паролей и т.д), но не полагайтесь полностью на него.

Узнайте, в каких соцсетях зарегистрирован ваш ребенок, просматривайте его страницу.

Поощряйте детей сообщать обо всем странном или отталкивающем и реагируйте спокойно, если что-то такое им действительно встретится.

Научите детей думать перед тем, как нажимать на любые кнопки и ссылки, особенно в электронных письмах.

7–8 лет

1. В этом возрасте еще можно требовать от ребенка соблюдения временных норм "экранного времени".
2. Включите в поисковиках фильтры безопасного поиска, блокировку сомнительных сайтов в браузере. Подключите функцию родительского контроля.
3. Подключите услуги блокировки платного контента, не кладите много денег на счет детского телефона. Убедитесь, что все ваши счета закрыты надежными паролями.
4. Создайте семейный электронный ящик: детям еще рано иметь собственные адреса.
5. Приучите детей советоваться с вами, прежде чем публиковать или скачивать что-либо.
6. Не забывайте беседовать с детьми об их друзьях в интернете, как если бы речь шла о друзьях в реальной жизни.
7. Расскажите детям про сайты "для взрослых" и их опасность.
8. Установите на все детские гаджеты качественные антивирусы от проверенных компаний.
9. Приучите ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом.
10. Обращайте внимание на возрастной рейтинг игр и приложений, которыми пользуется ребенок.

9–12 лет

1. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по интернету.
2. Приучите детей никогда не выдавать личную информацию в интернете без вашего разрешения. Аккаунты в соцсетях лучше вести под вымышленным именем и без фотографий.
3. Создайте ребенку ограниченную учетную запись для работы на компьютере.
4. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте и мессенджерам, чтобы вы убедились, что они не общаются с незнакомцами.
5. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.
6. Расскажите детям, что далеко не все, что они могут прочесть или увидеть в интернете – правда. Приучите их спрашивать о том, в чем они не уверены.
7. Расскажите детям о том, что публичный и школьный Wi-Fi может быть небезопасным, научите их подключаться через защищённый VPN-канал.
8. Установите ПО, которое может проверять и обновлять настройки конфиденциальности в социальных сетях.
9. Обсудите с ребенком опасный контент, с которым он может столкнуться: порнографию, пропаганду расовой ненависти, насилия и самоубийства.

13–17 лет

1. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.
2. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
3. Приучите себя знакомиться с сайтами, которые посещают подростки.
4. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.
5. Посоветуйте детям скачивать приложения только из официальных магазинов и избегать сомнительных P2P-источников.

” Невозможно всегда находиться рядом с ребенком и постоянно его контролировать. Доверительные отношения, доброжелательный диалог зачастую может быть гораздо конструктивнее, чем постоянное «отслеживание» посещаемых сайтов и блокировка контента.