МБОУ Калитвенская СОШ
Каменского района Ростовской области
Уполномоченный по правам ребенка

# Правила Интернет–безопасности (для взрослых и детей)

## Что такое информационная безопасность детей?

**Информационная безопасность детей** - это защита ребенка от дестабилизирующего воздействия информационной продукции и создания условий информационной среды для позитивной социализации и индивидуализации, оптимального социального, личностного, познавательного и физического развития, сохранения психического и психологического здоровья и благополучия, а также формирования позитивного мировосприятия. *(Распоряжение Правительства РФ от 02.12.2015 № 2471-р «Об утверждении Концепции информационной безопасности детей».)*

Как и в реальной жизни, подросток с Сети сталкивается с множеством проблем, в силу чего Интернет легко становится еще одним значимым источником стрессов в информационном обществе. Результаты исследований Фонда Развития Интернет, а также содержательный анализ более 5000 обращенийза трехлетний период работы горячей линии помощи «Дети онлайн» позволили выявить основные риски онлайн-среды для детей. Разработанная на этой основе классификация включает четыре типа рисков: контентные, коммуникационные, потребительские, технические.

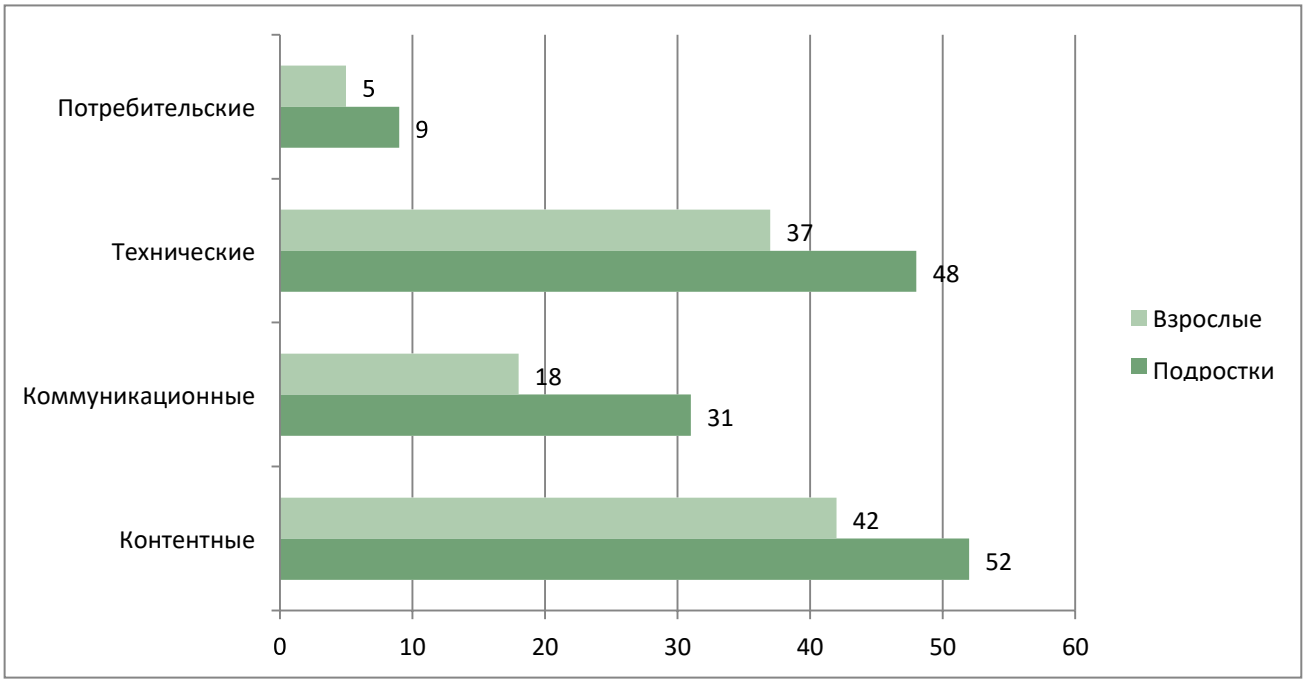


Диаграмма 1. Столкновение подростков с онлайн-рисками разных типов, %
*Выборка:* подростки 12-17 лет, пользующиеся Интернет; родители подростков 12-17 лет, пользующиеся Интернет

В целом, наиболее часто подростки сталкиваются с риском контентного (52%) и технического (48%) типа (Диаграмма 1).

Среди **контентных** рисков наиболее распространены сексуальные изображения и информацию с насилием, жестокостью или убийствами. Среди **технических** – вредоносные программы.

Именно об этих типах рисков наиболее осведомлены родители: каждый третий родитель знает, что его ребенок сталкивался с каким-либо из них (42% знают о контентных рисках, 37% - о технических). Хотя среди **технических** рисков родителям лучше всего известно о вирусах, а вот о взломах аккаунтов их детей знает только каждый шестой. В то же время каждый четвертый подросток жаловался на взлом его аккаунта в социальной сети или электронной почте.

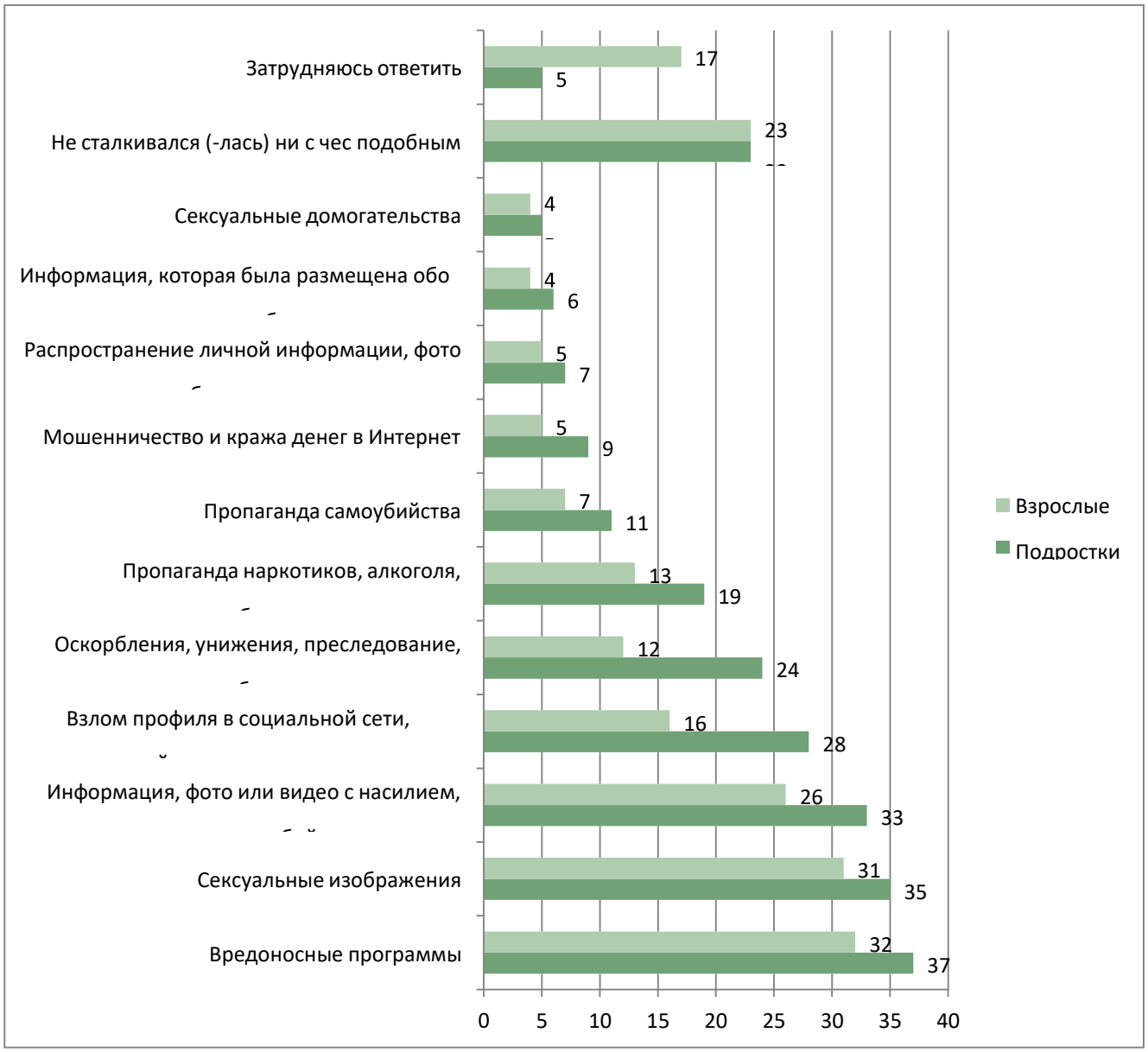


Диаграмма 2. С чем сталкивались подростки за последний год: сравнение оценок детей и родителей, %
*Выборка:* подростки 12-17 лет, пользующиеся Интернет; родители подростков 12-17 лет, пользующиеся Интернет

Практически каждый третий подросток сталкивался с **коммуникационными** рисками, однако родителей, которые знают о таком опыте своих детей, почти в 2 раза меньше. Среди коммуникационных рисков лидирует **кибербуллинг** (см. стр. 8) – каждый четвертый подросток указал, что за последний год сталкивался с оскорблениями, унижениями или преследованием в сети Интернет, но в курсе оказывается только один родитель из десяти (Диаграмма 2).

Мальчики немного чаще, чем девочки, сталкивались с пропагандой наркотиков, табакокурения или алкоголя, вредоносными программами и мошенничеством в Интернет, а также с тем, что их личная информация в социальных сетях была использована против них.

С возрастом дети сталкиваются с онлайн-рисками все чаще. Если каждый третий ребенок 12-13 лет не встречался ни с одним из перечисленных рисков, то в возрастной группе 16-17-летних только каждый десятый подросток смог избежать столкновения с Интернет-угрозами. В то же время, каждый шестой родитель не осведомлен о негативном опыте своего ребенка (Диаграмма 2).

Таким образом, самые частые проблемы в Интернет – вредоносные программы, контент, связанный с насилием, сексуальные изображения. Несколько реже подростки отмечают оскорбления, унижения, преследования, пропаганду наркотиков, алкоголя, табакокурения, взлом профиля. Причем каждый пятый подросток не сталкивался ни с чем из перечисленного. Представления родителей хотя и близки ответам подростков, но «отстают» по всем пунктам – т.е. родители недооценивают реальную ситуацию.

## К каким негативным последствиям может привести непрерывное продолжительное пребывание в сети Интернет?

Бесконтрольное распространение нежелательного контента противоречит целям образования и воспитания молодежи.

Отказываться от благ информационных технологий бессмысленно, но бесконтрольный доступ детей к сети Интернет может привести:

– к киберзависимости (патологической привязанности к компьютеру, невозможности оторваться от него ни на миг);

– к столкновению с вредоносными программами в сети Интернет (вирусы, шпионские программы, «боты» и т.п.);

– к нарушению нормального развития ребенка (синдром деформации внимания;гиперактивность, возникающая под влиянием информационной насыщенности, и др.);

– к неправильному формированию нравственных ценностей;

– к знакомству с человеком, у которого недобрые намерения (кибербуллинг, груминг, кибермошенничество).

## Как защитить свои персональные данные в сети Интернет?

**Персональные данные -** информация о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность.

Таких идентифицирующих данных огромное множество, к ним относятся: фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и прочее.

Для того чтобы не стать жертвой мошенников, необходимо руководствоваться следующими правилами.

Ограничьте объем информации о себе, находящейся в сети Интернет, удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию;

Не отправляйте видео и фотографии людям, с которыми вы познакомились в сети Интернет и не знаете их в реальной жизни;

Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат – действительно тот, за кого себя выдает;

Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы,класса и иные данные, посоветуйтесь с родителями или взрослым человеком, которому выдоверяете;

Используйте только сложныепароли, разные для разных учетных записей и сервисов;

Старайтесь периодическименять пароли;

Заведите себе два адреса электронной почты – частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный – для открытой деятельности (форумов, чатов и т.д.).

## Как защитить ребенка от нежелательного контента в сети Интернет?

К контентным рискам относятся 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.

**Противозаконный контент** - распространение наркотических веществ через Интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям.
**Вредоносный (опасный) контент** - контент, способный нанести прямой вред психическому и физическому здоровью детей и подростков.
**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, посвященные наркотикам, сайты, на которых размещены полные ненависти сообщения, 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.
**Предупреждение контентных рисков.**
Используйте специальные технические средства, чтобы ограничивать доступ ребенка к негативной информации – программы родительского контроля и контентной фильтрации, настройки безопасного поиска. Часто пакет функций родительского контроля уже есть в вашей антивирусной программе.
Программы родительского контроля позволяют: установить запрет на посещения сайтов различного негативного содержания, сайтов онлайн-знакомств, сайтов с вредоносным содержимым, ограничить время доступа ребенка к
Интернет, производить мониторинг переписки в социальных сетях и онлайн мессенджерах(чатах), блокировать сомнительные поисковые запросы в поисковых системах, блокировать баннеры, а также отслеживать все действия ребенка в сети.
Если ребенок пользуется общим компьютером, для каждого члена семьи создайте свою учетную запись на компьютере. Ваша учетная запись должна иметь надежный пароль и обладать правами администратора, чтобы ребенок не мог менять установленные вами настройки и программы.
Регулярно следите за активностью вашего ребенка в сети. Просматривайте историю посещений сайтов, чтобы быть уверенным, что
среди них нет опасных, при необходимости обновляйте настройки технических средств безопасности.
Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернет – правда. Необходимо проверять информацию, увиденную в Интернет.

Для этого существуют определенные правила проверки достоверности информации. Признаки надежного сайта, информации которого можно доверять, включают: авторство сайта, контактные данные авторов, источники информации, аккуратность представления информации, цель создания сайта, актуальность данных.
Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе, с какой информацией он сталкивается в сети. Попав случайно на какой-либо опасный, но интересный сайт, ребенок может продолжить поиск подобных ресурсов. Важно заметить это как можно раньше и объяснить, ребенку, чем именно ему грозит просмотр подобных сайтов.

## Как научить ребенка быть осторожным при знакомстве с новыми людьмив сети Интернет?

Общение в сети Интернет может повлечь за собой коммуникационные риски,такие как: груминг, кибербуллинг и т.д.
Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье. Также юный пользователь рискует подвергнуться оскорблениям, запугиванию и домогательствам. Особенно опасным может стать **груминг** – установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации. Такие знакомства чаще всего происходят в чате, на форуме или в социальной сети. Общаясь в сети Интернет, злоумышленник, чаще всего представляясь сверстником, входит в доверие к ребенку, а затем пытается узнать личную информацию (адрес, телефони др.) и договориться о встрече. Иногда такие люди выманивают у детей информацию, которой потом могут шантажировать ребенка, например, просят прислать личные фотографии или провоцируют на непристойные действия перед веб-камерой.

**Предупреждение груминга.**
Будьте в курсе, с кем контактирует в сети Интернет ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются.
Объясните ребенку, что нельзя разглашать в сети Интернет информациюличного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать Интернет-знакомым свои фотографии.

Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу.
Не позволяйте вашему ребенку встречаться с онлайн-знакомыми без вашего разрешения или в отсутствии взрослого человека.
Интересуйтесь тем, куда и с кем ходит ваш ребенок.

**Как противостоять грумингу.**

Если ребенок желает познакомиться с новым Интернет-другом, следует настоять на сопровождении ребенка на эту встречу.
Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию.
Сохраняйте спокойствие – вы можете напугать ребенка своей бурной реакцией на то, что он рассказал или показал. Главной задачей является эмоциональная поддержка ребенка. Нужно дать ребенку уверенность в том, что проблему можно преодолеть. Никогда не наказывайте и не ограничивайте действия ребенка в ответ на его признание.
Сохраните все свидетельства переписки и контактов незнакомца с ребенком (скриншоты экрана, электронные письма, фотографии и т.п.).
При обнаружении признаков совращения следует немедленно сообщить об этом в правоохранительные органы.
Повторите ребенку простейшие правила безопасности при использовании сети Интернет, дайте советы по дальнейшему предотвращению груминга.

**Кибербуллинг -** одна из форм преследования, травли, запугивания, насилия подростков и младших детей при помощи различных Интернет-сервисов.

**Предотвращение кибербуллинга.**

При общении в сети Интернет оставаться дружелюбным с другими пользователями. Не стоит писать резкие и оскорбительные слова – читать грубости также неприятно, как и слышать.
Научиться правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Возможно, стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем. Лучший способ испортить хулигану его выходку – отвечать ему полным игнорированием.
Не стоит в сети Интернет распространять о себе личную информацию (ФИО, год и дата рождения, адрес проживания, номер телефона и т.д.), выкладывать фотографии, так как данные сведения могут быть использованы агрессором против вас.

**Следует обратить внимание на ряд признаков в поведении ребенка, которые могут свидетельствовать о том, что подросток стал жертвой кибербуллинга.**

1. Беспокойное поведение. Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

2. Неприязнь к Интернет. Если ребенок любил проводить время в сети Интернет и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в сети Интернет.

3. Нервозность при получении новых сообщений. Негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

**Как справляться с кибербуллингом.**

Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию.

Сохраните все возможные свидетельства происходящего (скриншоты экрана, электронные письма, фотографии и т.п.).

Сохраняйте спокойствие – вы можете еще больше напугать ребенка своей бурной реакцией на то, что он вам рассказал и показал. Главной задачей является эмоциональная поддержка ребенка. Нужно дать ему уверенность в том, что проблему можно преодолеть. Никогда не наказывайте и не ограничивайте действия ребенка в ответ на его признание.

Повторите ребенку простейшие правила безопасности при использовании сети Интернет, дайте советы по дальнейшему предотвращению кибербуллинга.

## Как научить ребенка не стать жертвой Интернет-мошенников?

**Кибермошенничество** - один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.) с целью причинить материальный или иной ущерб.

**Предупреждение кибермошенничества.**

Проинформируйте ребенка о самых распространенных методах мошенничества в сети. Всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в сети Интернет.

Не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать покупки.

Не отправляйте о себе слишком много информации при совершении Интернет-покупок (данные счетов, пароли, домашние адреса и телефоны). Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.

Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.

Убедитесь в безопасности сайта, на котором вы и ваш ребенок планируете совершать покупку (ознакомьтесь с отзывами покупателей, избегайте предоплаты, проверьте реквизиты юридического лица – владельца магазина,

уточните, как долго существует магазин, поинтересуйтесь возможностью получения кассового чека и других документов на покупку, сравните цены в различных Интернет-магазинах, позвоните в справочную магазина, обратите внимание на правила Интернет-магазина, выясните, сколько точно вам придется заплатить).

## Как предупредить столкновение с вредоносными программами в сети Интернет?

**Вредоносные программы** - различное программное обеспечение (вирусы, черви, «троянский конь», шпионские программы, «боты» и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обменаданными с Интернет, 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 Интернет файлов.

**Предупреждение столкновения с вредоносными программами**

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.

Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.

Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.

Следите за тем, чтобы ваш антивирус регулярно обновлялся, и раз в неделю проверяйте компьютер на вирусы.

Регулярно делайте резервную копию важных данных, а также научите это делать ваших детей.

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.).

Объясните ребенку, что нельзя рассказывать никакие пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.

Предупредите ребенка о том что если он пользуется Интернет 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 программного обеспечения или в технический сервис.

## Как не стать Интернет-зависимым?

**Интернет-зависимость** - навязчивое желание войти в Интернет, находясь офлайн и неспособность выйти из Интернет, будучи онлайн.

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 Интернет, связанными с общением. Другую часть зависимых (9%) привлекают информационные сервисы сети.

**Предупреждение Интернет-зависимости.**

Оцените, сколько времени ваш ребенок проводит в сети Интернет, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.

Поговорите с ребенком о том, чем он занимается в Интернет. Социальные сети создают иллюзию полной занятости — чем больше ребенок общается, тем большеу него друзей, тем больший объем информации ему нужно охватить — ответить на все сообщения, проследить за всеми событиями, показать себя. Выясните,

поддерживается ли интерес вашего ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать, насколько важно для ребенка общение в сети Интернет и не заменяет ли оно реальное общение с друзьями.

Понаблюдайте за сменой настроения и поведения вашего ребенка после выхода из Интернет. Возможно проявление таких психических симптомов, как: подавленность, раздражительность, беспокойство, нежелание общаться. Из числа физических симптомов можно выделить: головные боли, боли в спине, расстройства сна, снижение физической активности, потеря аппетита и др.

Поговорите со школьным психологом и классным руководителем о поведении вашего ребенка, его успеваемости и отношениях с другими учениками. Настораживающими факторами являются замкнутость, скрытность, нежелание идти на контакт. Узнайте, нет ли у вашего ребенка навязчивого стремления выйти в Интернет с помощью телефона или иных мобильных устройств во время урока.

**Как справляться с Интернет-зависимостью.**

Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и т.д.


Не запрещайте ребенкупользоваться Интернет, но постарайтесь установить регламент пользования (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения домашних уроков и пр.). Для этого можно использовать специальные программы родительского контроля, ограничивающие времяв сети Интернет.

Ограничьте возможностьдоступа к Интернет только своим компьютером или компьютером, находящимся в общей комнате — это позволит легче контролировать деятельность ребенка в сети Интернет. Следите за тем,какие сайты посещает ваш ребенок.

Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в Интернет. Это поможет наглядно увидеть и осознать проблему, а также избавиться от некоторых навязчивых действий - например, от бездумного обновления странички в ожидании новых сообщений.

Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибердеятельность в реальную жизнь. Например, для многих компьютерных игр существуют аналогичные настольные игры, в которые можно играть всей семьей или с друзьями, при этом общаясь друг с другом «вживую». Важно, чтобы у ребенка были не связанные с Интернет увлечения, которым он мог бы посвящать свое свободное время.

Дети с Интернет-зависимостью субъективно ощущают невозможность обходиться без сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без Интернет. Важно, чтобы ребенок понял — ничего не произойдет, если он на некоторое время «выпадет» из жизни Интернет-сообщества.
В случае серьезных проблем обратитесь за помощью к психотерапевту.

***Уважаемые родители!***

***Важно помнить, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения, открытый и доброжелательный диалог с детьми зачастую могут выступать более эффективными средствами для обеспечения безопасности вашего ребенка,чем постоянное отслеживание посещаемых сайтов и блокировка***

## Полезные телефоны и Интернет-ресурсы

***Дети России Онлайн:*** http://detionline.com

***Линия помощи «Дети Онлайн»***
**тел.:** 8-800-25-000-15 (звонок по России бесплатный).
**e-mail:** helpline@detionline.com

***Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникации:*** http://rkn.gov.ru

***Лига безопасного Интернета:*** http://www.ligainternet.ru

***Мониторинговый центр по выявлению опасного и запрещенного законодательством контента:*** http://www.pedofilov.net

***Проект Microsoft. «Безопасность детей в Интернет». Правовые, психологические, технические аспекты безопасной работы в Интернет:***
http://krkam.edusite.ru/DswMedia/proektmicrosoftobezopasnostideteyvinternet.pdf

Подготовила уполномоченный по правам ребенка Желтова О. А.