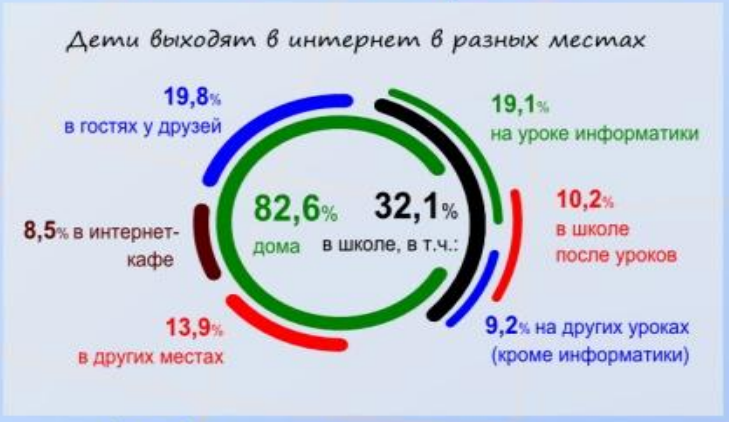
БЕЗОПАСНОСТЬ В СЕТИ

7 из 10 детей (72,2%)
Часто пользуются интернетом

Дети выходят сеть из разных мест

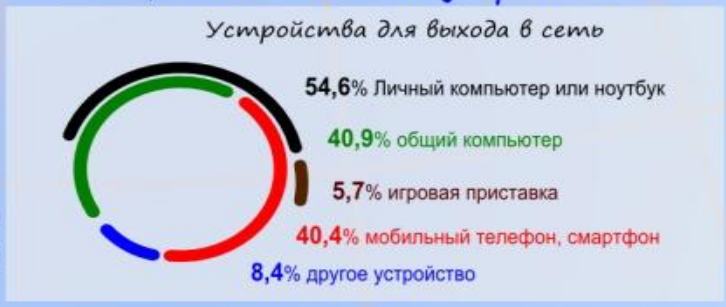


8 из 10 детей (82,6%)
выходят в интернет из дома

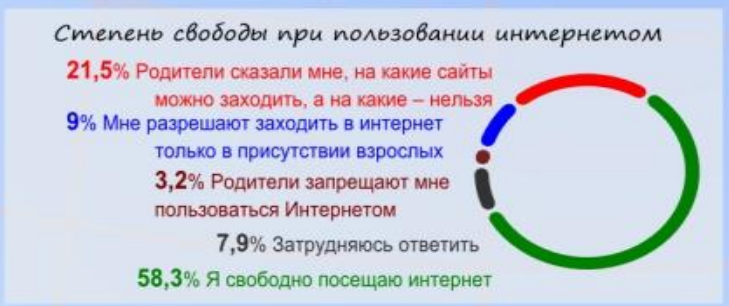
Каждый 3-й ребенок (32,1%) выходит в интернет в школе, и не только на уроках (10,2%)

40,4% детей выходят в сеть с помощью своих мобильных устройств

Большая часть детей использует собственный компьютер или ноутбук



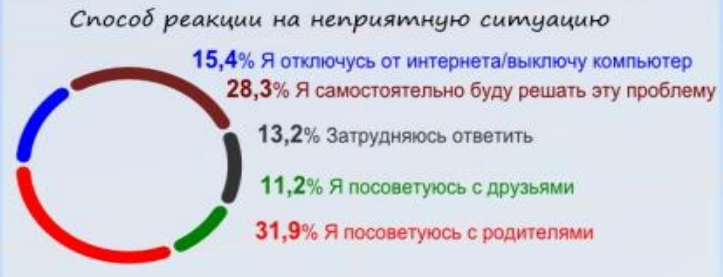
Больше половины детей (58, 3%) свободно посещают любые сайты



Каждому 30-му ребенку родители запрещают интернет

Только 39,1% детей в случае возникновения неприятной ситуации в интернете обратятся к родителям за советом и помощью

Около четверти несовершеннолетних (28,3%) проявляют самостоятельность при разрешении неприятных ситуаций



Ваш ребенок снова «прилип» к монитору... Особенно эта проблема актуальна в дни школьных каникул – родители на работу, а ученик – «зависать» в сети. Тревожная статистика показывает, что каждый пятый подросток (21,9%) подвергался виртуальному террору - кибербуллингу. Как помирить ребенка с компьютером, оградив его от «взрослых сайтов» и нежелательной активности со стороны сверстников?

Исследование об интернет-зависимости среди европейских детей 14-17 лет показало, что почти у всех (92%) подростков, которые регулярно используют интернет, есть зарегистрированные профили как минимум в одной социальной сети. Как свидетельствует еще один опрос, проведенный среди европейской молодежи, почти 75% опрошенных латвийских подростков используют подключение к интернету в любом месте, где бы они ни находились. Больше половины (63%) европейской молодежи признались, что в сети они общаются с незнакомцами, а каждый третий из них встречался с ними лично.

Еще одна проблема – **кибербуллинг**. Как отметил независимый эксперт, IT-блогер Кристапс Скутелис, еще лет 20 назад дети спорили на игровых площадках, а теперь в виртуальной среде, преимущественно в социальных сетях.

Мнение разделяет главный научный сотрудник по безопасности в «Лаборатории Касперского» Дэвид Эмм. В беседе с «Гранями» он подчеркнул, школьники предпочитают «вести войну» друг с другом с помощью современных технологий и интернета. К примеру, используют смартфоны, чтобы сфотографировать кого-то из одноклассников в раздевалке, а затем выложить фото в Facebook для привлечения всеобщего внимания. Как правило, одноклассники активно делятся такими фотографиями со всей школой, чтобы посмеяться над несчастной жертвой. Европейское исследование, проведенное среди подростков 14-17 лет, привело к тревожным выводам - каждый пятый подросток в Европе испытывал на себе запугивания и издевательства в интернете.

- Виртуальный террор ни в коем случае нельзя считать пустяковым явлением, - поясняет Дэвид Эмм. - Более половины опрошенных школьников (53,5%), которые испытали это на себе, указали, что запугивания и издевательства в интернете очень негативно сказались на их психике. Интересно, что жертвами подросткового кибербуллинга становятся как мальчики, так и девочки, однако девочек атакуют чаще.

В многогранном виртуальном мире полезная информация перемежевывается с чернухой, порнографией. А еще здесь можно встретить преступников, которые, играя на доверчивости детей, могут опустошить родительский кошелек, предлагая поучаствовать в различных конкурсах, викторинах и т.д., позвонив по платному телефону или заплатив кредиткой. Что делать?

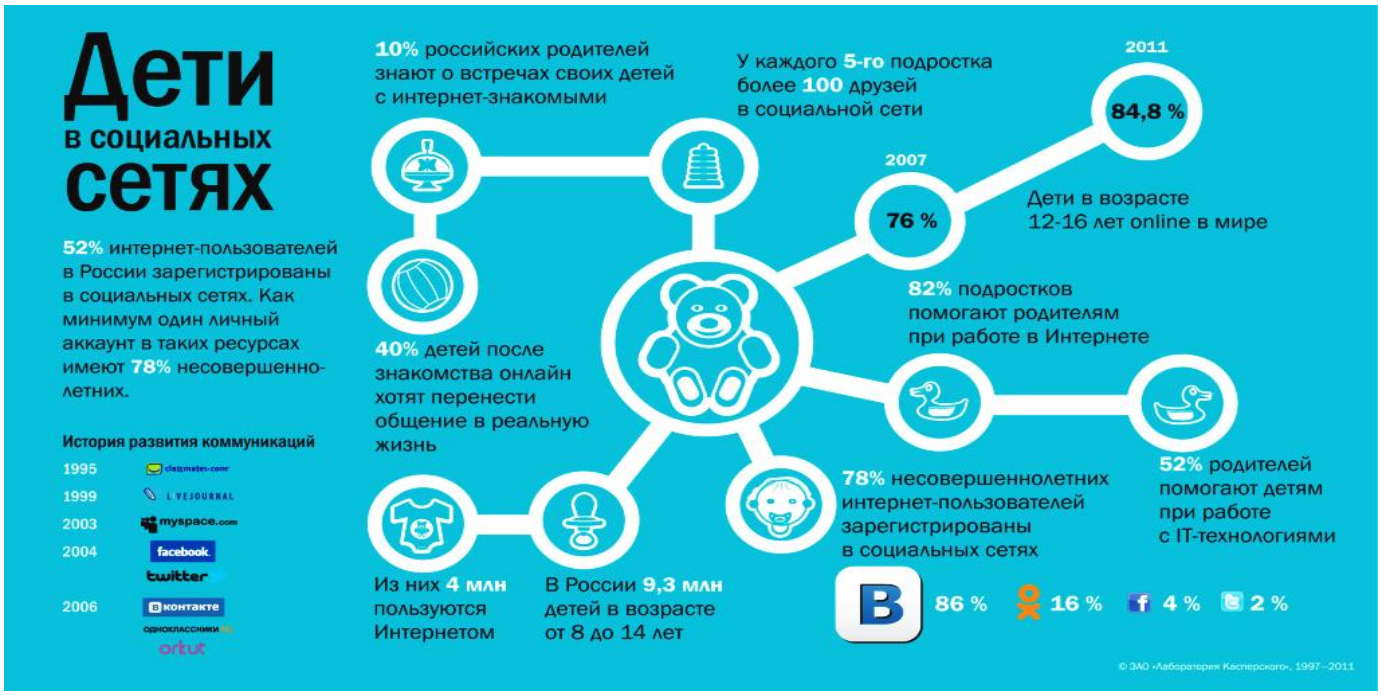
Как отмечают специалисты, существует два подхода к решению проблемы: технический и психологический.

- В наш век высоких технологий запрещать компьютер глупо, - убеждена психолог-практик Евгения Карлин. - Установите лимит времени за компьютером и предложите альтернативу. Ни в коем случае не дополнительные задания по школьной программе, чтение или уборку, а то, что могло бы заинтересовать ребенка: игры, поездки, совместное творчество и пр. Помимо «дозировки» общения, обратите внимание, дети наивно относятся к общению в Сети. Расскажите о возможных опасностях. Установите правила пользования компьютером, например, спрашивать разрешения, прежде чем скачивать какую-либо информацию, чтобы избежать откровенных материалов сексуального характера. Целесообразно также установить программы защиты. Это не пуританские пережитки. **Ребенок может принять порнографию за жестокую норму, либо просмотр сцен может оказать серьезную психологическую травму, в дальнейшем повлиять на сексуальное развитие. Даже подросткам, информированным о сексе, порнография наносит вред, не является способом сексуального просвещения. Кроме того, существует проблема психологической зависимости от порнографии, которая также оказывает негативное влияние на психику и сексуальность.**

Как оградить ребенка от «непрошенных гостей» из интернета? Рекомендуют латвийские специалисты IT-технологий.

1. Первые шаги в Сети детям лучше делать вместе со взрослыми, которые на примерах расскажут о возможных опасностях.
2. Сформулируйте, какую информацию можно публиковать в интернете, а какую нет (личные данные, домашний адрес, фотографии квартиры, новости о семейных покупках и т.д.). Часто эти данные являются «пособием для преступников».
3. Ребенок должен усвоить: предложения о бесплатных подарках и легком заработке, как правило, распространяют злоумышленники.

4. Киберпреступники самыми разными путями пытаются выманить у доверчивых пользователей данные кредитных карт. Поэтому ребенок должен рассчитываться в интернете под контролем взрослых.
5. Чтобы защитить своего ребенка от неприятных последствий использования компьютеров и смартфонов, родители могут использовать соответствующие приложения «Родительский контроль» (их предлагают разработчики антивирусных программ и производители мобильных телефонов).



Возможные негативные моменты, с которыми приходилось сталкиваться :

- страх признаться об определенных действиях в интернете или их последствиях может привести к попыткам суицида или уходу из дома (платные ресурсы с отправкой смс, заражение компьютера блокировщиками системы)
- шантаж с требованием денег, продолжением действий или встречей в реале со стороны кибер-злодеев, в случае, если подросток в ходе общения отсылал фото или видео интимного или эротического содержания своему собеседнику
- отсылка детской порнографии детям и подросткам, уговоры наблюдать за мастурбацией извращенца, предложение реального и виртуального секса за деньги или за виртуальные статусы
- организация провокаций межэтнического характера с участием молодежи

Как помочь вашим детям более безопасно пользоваться сайтами социальных сетей

Сегодня многие дети не делают различий между реальной жизнью и виртуальной жизнью в Интернете. Они могут пользоваться сайтами социальных сетей, предназначенных для детей, такими как Webkinz или Club Penguin, или сайтами социальных сетей, предназначенных для взрослых, такими как Windows Live Spaces, YouTube, MySpace, Flickr, Twitter, Facebook и другими. Что бы они не делали, они должны понимать, что многие из этих веб-страниц могут просматривать кто угодно, кто обладает доступом в Интернет.

Дети могут использовать эти сайты для: чата; игр; публикации и просмотра фотографий и видео;

Блог, публикации профиля в Интернете.

К сожалению, часть информации, которые дети публикуют на своих страницах, может также делать их уязвимыми для фишинговых сообщений,киберугроз и интернет-похитителей. Далее описано несколько способов, как вы можете помочь детям более безопасно пользоваться сайтами социальных сетей.

Поговорите с детьми об опыте их общения в социальных сетях. Попросите детей рассказывать вам, если они столкнутся на этих сайтах с чем-либо, что вызывает у них беспокойство, неудобство или страх. Проявляйте спокойствие и напомните детям, что их никогда не накажут за то, что они вам расскажут. Дайте детям понять, что вы вместе с ними постараетесь найти удачный выход из сложившейся ситуации.

Установите собственные правила пользования Интернетом у вас дома Как только дети начнут самостоятельно пользоваться Интернетом, желательно подготовить список правил пользования Интернетом, которые будут приняты всеми. В этих правилах должно быть указано, могут ли дети использовать сайты социальных сетей и каким образом. Для получения дополнительных сведений о том, как установить правила, см. Использование семейных контрактов для защиты детей в Интернете.

Проследите за тем, чтобы дети соблюдали возрастные ограничения на сайте. Рекомендуемый возраст для регистрации на сайтах социальных сетей обычно составляет 13 или более лет. Если ваши дети не достигли рекомендуемого возраста, указанного для данных сетей, не разрешайте им пользоваться сайтами. Важно помнить, что вы не должны полностью полагаться на службы сайта, которые не допускают регистрации детей, не достигших нужного возраста.

Научитесь пользоваться сайтом. Оцените сайты, которые планирует использовать ваш ребенок, и убедитесь, что вы и ваш ребенок понимают политику конфиденциальности и правила поведения. Узнайте, существует ли на сайте контроль над публикуемым содержимым. Кроме того, периодически просматривайте страницу вашего ребенка. Для получения дополнительных предложений см. Советы по безопасному ведению блогов для детей и родителей.

Настаивайте на том, чтобы дети никогда лично не встречались с тем, с кем они общались только по Интернету, и просите их общаться только с теми, кого они знают лично. Дети подвергаются реальной опасности во время личной встречи с незнакомыми людьми, с которыми они общались только по сети. Вы можете защитить своих детей, попросив их общаться в Интернете со своими друзьями и не общаться с теми, с кем они лично не встречались.

Иногда бывает недостаточно просто сказать детям, чтобы они не разговаривали с незнакомыми людьми, поскольку дети могут не считать незнакомым человека, с которым они «встречались» в сети. Для получения дополнительных советов по защите ваших детей в Интернете см. Интернет-преступники: что можно сделать, чтобы уменьшить риск.

Убедитесь в том, что ваши дети не указывают свои полные имена. Проследите за тем, чтобы дети использовали только свои имена или псевдонимы, но никогда не использовали псевдонимы, которые бы вызывали ненужное внимание. Кроме того, не разрешайте своим детям публиковать полные имена своих друзей.

Опасайтесь наличия в профиле ребенка информации, по которой можно идентифицировать его личность. На многих сайтах социальных сетей дети могут присоединяться к общественным группам, включающих учеников определенной школы.

Будьте бдительны, если дети разглашают эту и другую информацию, которую можно использовать для их идентификации, например школьный питомец-талисман, рабочие места и название города проживания. Если указано слишком много информации, ваши дети могут подвергаться киберугрозам, атакам со стороны интернет-преступников, интернет-мошенников или краже личных данных.

Постарайтесь выбрать сайт, который не столь широко используется. Некоторые сайты позволяют защитить вашу страницу с помощью пароля или другими способами, чтобы ограничить круг посетителей, разрешив его только тем лицам, которых знает ваш ребенок. Например, с помощью Windows Live Spaces вы можете настроить разрешения, указав тех, кто может посещать ваш сайт. При этом возможны самые различные настройки – от всех пользователей Интернета до ограниченного списка людей.

Следите за деталями на фотографиях. Объясните детям, что фотографии могут раскрывать много личной информации. Попросите детей не публиковать фотографии себя или своих друзей, на которых имеются четко идентифицируемые данные, такие как названия улиц, государственные номера автомобилей или название школы на одежде.

Предостерегите своего ребенка относительно выражения своих эмоций перед незнакомцами. Вероятно, вы уже предупреждали своих детей не общаться с незнакомыми людьми напрямую по сети. Однако дети

используют сайты социальных сетей для написания журналов и стихотворений, в которых часто выражают сильные чувства. Объясните детям, что многое из публикуемого сможет прочесть любой пользователь, имеющий доступ в Интернет, а также что похитители часто ищут эмоционально уязвимых детей. Для получения дополнительной информации см. Чему следует научить детей, чтобы повысить их безопасность при работе в Интернете.

Расскажите детям об интернет-угрозах. Как только ваши дети станут достаточно взрослыми для использования социальных сетей, поговорите с ними о киберугрозах. Расскажите детям, что если у них возникнет ощущение, что им угрожают через Интернет, то им сразу же следует сообщить об этом родителям, учителю или другому взрослому человеку, которому они доверяют. Кроме того, очень важно научить детей общаться по сети точно так же, как они общаются лично. Попросите детей относиться к другим людям так же, как они хотели бы, чтобы относились к ним самим.

Удаление страницы вашего ребенка. Если ваши дети откажутся следовать установленным правилам, которые предназначены для их безопасности и вы безуспешно пытались их убедить следовать им, то вы можете обратиться на сайт социальной сети, который использует ваш ребенок, и попросить удалить его страницу. Можно также обратить внимание на средства фильтрации интернет-содержимого в качестве дополнения и ни в коем случае не замены для контроля со стороны родителей.

Что делать, если кто-то угрожает вашему ребенку через Интернет

Лучшая поддержка для ребенка, которому угрожают через Интернет, – это позитивная, активная, компетентная и предсказуемая поддержка.

Действуйте немедленно. Ваш ребенок должен знать, что вы можете ему помочь и обязательно поможете ему. Не дожидайтесь, пока оскорбления прекратятся. Если вы чувствуете, то ваш ребенок физически подвергается риску, сразу же обратитесь в полицию.

Должны быть предприняты все усилия, чтобы найти киберпреступника и привлечь его или ее к ответственности. Если преступником является ученик, можно сообщить об этом в школу. Сообщите об угрозах на веб-сайт, где вывешиваются угрозы. Для многих служб имеются модераторы и адреса, по которым следует сообщать о фактах угроз и оскорблений. Обратитесь в сотовую компанию и попросите отследить вызов и предпринять соответствующие меры.

Попросите детей не отвечать на киберугрозы и не мстить за них, поскольку хулиганы ожидают реакцию. Не отвечайте на телефонные звонки и не отвечайте (или даже не читайте) на текстовые сообщения или комментарии.

Блокировка киберхулиганов. Большинство веб-служб позволяют блокировать тех пользователей, которые ведут себя неподобающим образом или каким-либо образом угрожают. Обратитесь в соответствующую службу — в социальную сеть, компанию мгновенных сообщений, оператору сотовой связи, чтобы выяснить, как можно противостоять этой угрозе.

Сохраните доказательства. Сохраните текстовые сообщения, сообщения электронной почты и другие доказательства киберугроз на случай, если они потребуются правоохранительным органам.

Каким образом действуют интернет-преступники?

Интернет-преступники действуют следующим образом:

- находят детей через социальные сети, блоги, чат-комнаты, мгновенные сообщения, по электронной почте, через доски обсуждений и другие сайты.
- Заманивают потенциальные жертвы, оказывая знаки внимание, проявляя доброту, ласку и даже с помощью подарков.
- Знают современную музыку и хобби, которые могут заинтересовать детей.
- Прислушиваются и симпатизируют проблемам детей.
- Стараются смягчить запретные барьеры для молодежи, постепенно вводя сексуальные темы в разговоры или показывая откровенные сексуальные материалы.
- Также могут оценивать детей, которых они встречают в сети, для будущих личных контактов.

Как родители могут уменьшить риск того, что их ребенок станет жертвой?

Поговорите с детьми о сексуальных преступниках и потенциальных опасностях в сети.

Используйте программное обеспечение родительского контроля, которое встраивается в новые операционные системы, например Windows 7 или Windows Vista , или которое можно загрузить бесплатно, например Параметры семейной безопасности Windows Live.

Соблюдайте возрастные ограничения на сайтах социальных сетей. Большинство сайтов социальных сетей требуют, чтобы возраст пользователей составлял 13 и более лет. Если возраст ваших детей меньше рекомендуемого, не разрешайте им использовать эти сайты.

Маленькие дети не должны пользоваться чат-комнатами — опасность очень велика. Когда дети повзрослеют, направьте их в хорошо контролируемые детские чат-комнаты. Попросите своих детей-подростков пользоваться контролируемыми чат-комнатами.

Если ваши дети участвуют в электронном общении, обязательно узнайте, какие чат-комнаты они посещают и с кем общаются. Самостоятельно контролируйте области чата, чтобы следить за тем, какого рода разговоры там происходят.

Проинструктируйте детей никогда не покидать область общего пользования чат-комнаты. Многие чат-комнаты предлагают области для личного общения, где пользователи могут общаться один на один с другими пользователями, и служба мониторинга не может читать эти сообщения. Часто они называются областями "шепота".

Компьютеры, подключенные к Интернету, должны находиться в открытом месте, а не в спальне ребенка-подростка. Преступнику намного сложнее установить отношения с вашим ребенком, если экран компьютера хорошо просматривается. Даже если компьютер находится в зоне общего пользования у вас дома, находитесь рядом с детьми, когда они подключаются к Интернету.

Когда дети маленькие, они должны использовать семейный адрес электронной почты, а не заводить собственные адреса. По мере того, как они будут становиться взрослее, попросите своего поставщика электронной почты настроить отдельный адрес электронной почты, однако почта ваших детей должна по-прежнему находиться внутри вашей учетной записи.

Скажите детям никогда не отвечать на мгновенные сообщения или сообщения электронной почты от незнакомцев. Если ваши дети используют компьютеры, которые вы не можете контролировать – в общественной библиотеке, в школе, дома у друзей, - выясните, какие средства защиты компьютера там используются.

Если все меры предосторожности не помогли и ваши дети все же встретились с интернет-преступником, не ругайте их. Обидчик всегда несет полную ответственность. Предпримите решительные действия, чтобы прекратить дальнейшие контакты вашего ребенка с этим человеком.

Как дети могут снизить риск стать жертвой?

Существует несколько мер предосторожности, которые дети должны соблюдать, включая:

Никогда не загружать фотографии из неизвестного источника. Они могут иметь сексуально откровенный характер.

Использовать фильтры электронной почты..

Немедленно рассказывать взрослым, если во время работы в Интернете произойдет что-то, что вызывает неудобство или страх.

Выбрать нейтральное имя, которое не содержит указания на пол и не раскрывает личную информацию.

Никогда не разглашать личную информацию о себе (включая возраст и пол), а также информацию о своей семью, никогда не заполнять личные анкеты в Интернете. Для получения более подробных правил относительно использования личной информации на таких сайтах, как Windows Live Spaces или MySpace, см. Как помочь вашим детям более безопасно пользоваться сайтами социальных сетей.

Немедленно прекращать любое общение по электронной почте, с использованием мгновенных сообщений или чатов, если кто-то пытается задавать вопросы, являющиеся очень личными или имеющие сексуальную **направленность.**

Поместить соглашение семьи по использованию Интернета рядом с компьютером, которое бы напоминало детям о защите своей конфиденциальности в Интернете.

Что делать, если ваш ребенок стал объектом домогательств?

Если ваш ребенок получает сексуально откровенные фотографии от корреспондента в Интернете или если его или ее сексуально домогаются по электронной почте, с использованием мгновенных сообщений или иным способом с использованием Интернета, обратитесь в местную полицию. Сохраните все документы, включая адреса электронной почты, адреса веб-сайтов и журналы разговоров по сети, чтобы предоставить их полиции.

Проверьте наличие на своем компьютере порнографических файлов, а также любого рода сексуальных коммуникаций — очень часто они являются предупредительными сигналами.

Контролируйте доступ ребенка к любым электронным средствам интерактивной связи, таким как чат-комнаты, система обмена мгновенными сообщениями и электронная почта.

Куда обращаться:

В интернете: http://www.ligainternet.ru/hotline/

В Санкт-Петербурге, официальное подразделение: **отдел «К»** ГУ МВД СПБ и ЛО

Если столкнулись в Интернете с нарушением или преступлением или чем-то не совсем понятным, но вызывающем тревогу и если нет желания напрямую сразу обращаться в МВД, можно обратиться: **«Молодежная Служба Безопасности»**, www.molbez.ru (любые проблемы, связанные с молодежью, преступностью и пр., если нет доверия к официальным структурам; проводится анализ информации и адресный «подбор» профильных проверенных сотрудников правоохранительных органов для работы по проблеме). Также можно обратиться непосредственно к руководству «МСБ»: https://vk.com/helpersaver или msb-21@mail.ru