

методическая разработка

«Безопасность детей в Интернет»

«Безопасность детей в Интернет»

Тема 1. Преступники в Интернет.

Цель: формирование представлений об опасностях, с которыми могут столкнуться дети при общении по сети Интернет.

План лекции:

1. Преступные действия, которым может подвергнуться ребенок в сети Интернет.
2. Ребенок стал потенциальной жертвой преступника. Действия взрослых.

Скорость распространения информационных технологий в наши дни становится все стремительнее. Сегодня мы говорим уже о 600 миллионах пользователей персональных компьютеров, и в ближайшей перспективе эта цифра может превысить 1 миллиард. Компьютер широко используется не только на рабочем месте, но и в быту, дома, на отдыхе. Причем для домашнего использования персональные компьютеры приобретаются в гораздо больших объемах, нежели для организаций. Это общемировая тенденция, и наша страна не является здесь исключением.

Число пользователей Интернета в России стремительно растет, причем доля молодежи и совсем юной аудитории среди пользователей Всемирной паутины очень велика. Информационно-коммуникационные технологии (ИКТ) предоставляют беспрецедентные возможности для детско-юношеского обучения и творчества. Для многих, особенно молодых людей, Интернет становится информационной средой, без которой они не представляют себе жизнь. И это неудивительно, ведь в Интернете можно найти информацию для реферата, послушать любимую мелодию, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах. В то же время серьезной проблемой во всем мире стало злоупотребление плодами ИКТ и использование их для совершения преступлений против детей.

Сеть тоже может быть опасна. В ней появились своя преступность, хулиганство, вредительство, порнография, терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое — яркие примеры контента, с которым могут соприкоснуться дети и подростки. К настоящему времени проблема безопасности детей в Интернете, без преувеличения, стала глобально значимой проблемой. **Спам, кибермошенничество, коммуникационные риски, незаконный контакт, киберпреследование, блокирование доступа к неподходящим материалам** — только некоторые из опасностей подстерегающих детей в сети Интернет.

Почтовый спам не только способен досаждать пользователя назойливой и непрошенной рекламой, вызывая ряд неудобств, связанных главным образом с потерей времени на очистку почтового ящика. Подобные рекламные сообщения зачастую несут в себе и угрозу для работоспособности

персонального компьютера и сохранности конфиденциальных данных. Дело в том, что все чаще в почтовые ящики падают письма с ссылками, ведущими на небезопасные сайты, и «зараженными» вложенными файлами. Спамерская рассылка, на которую приходится от 70 до 80% всех писем, все чаще несет в себе не рекламу товаров и услуг, а скрытые трояны и вирусы.

Интернет-мошенничество и кража личных данных может произойти, если ребенок отвечает на спам-сообщения или на его компьютер была запущена какая-либо вредоносная программа, позволившая хакеру получить к нему доступ.

Киберпреследование – еще один вид преступления в сети. Орудиями киберпреследователя являются электронная почта, мессенджеры (например, ICQ), форумы и чаты, а теперь еще и социальные сети – не говоря уже о SMS и MMS. Сеть позволяет злоумышленнику остаться анонимным. Вычислить преследователя без применения специальных средств очень сложно, а в ряде случаев почти невозможно. Типичное киберпреследование выглядит так: все контакты ребенка начинают заваливать сообщениями примерно одной и той же направленности. В отличие от спама, шлют эти сообщения вполне. Для этого киберпреследователь собирает информацию об электронных контактах ребенка как из публичных источников, например, соцсетей, так и из личных, например, троянами или через знакомых ребенка. Дальше он решает, по каким контактам атаковать. Обычно в таких случаях редко церемонятся и «берут в работу» все. Вред, причиняемый в результате киберпреследования, каждый оценивает субъективно. В большинстве случаев это «паралич» всех электронных контактов жертвы и постоянное нервное напряжение. Иногда это приводит к тому, что в потоке теряются полезные сообщения или не может «пройти» действительно необходимая информация. Бывает, что доведенный до отчаяния человек полностью меняет свои контакты.

Особо тяжким случаем киберпреследования является длительное целенаправленное преследование жертвы злоумышленником-маньяком самыми разными способами. Преступник рассылает сообщения с угрозами причинения телесного вреда или убийства, терроризирует объект на любимых сайтах и социальных сетях. Например, он может опубликовать там реальные данные о жертве или клевету. Эти преследования часто переносятся в реальную жизнь: жертву начинают мучить телефонными звонками, записками с угрозами. Хорошо, если подобные вещи всего лишь «шутка», и преследователь не собирается воплощать их в жизнь. В любом случае, необходимо обратиться в милицию, так как преследование человека, нарушение его спокойной частной жизни является преступлением. И если злоумышленника удастся обнаружить, он понесет серьезное наказание независимо от того, насколько реальны были его угрозы.

Запугивание в Интернете легко осуществимо с технической точки зрения, поэтому заниматься им может даже невинный подросток. По данным США за 2008 год, 41% подростков сталкивались с угрозами по Интернету 1-3 раза в течение года. 13% опрошенных подвергались онлайн-овому запугиванию 4-6 раз за год, а 19% подростков — 7 раз и более. Половине из

них угрожали их одноклассники, в 43% случаев — онлайн-знакомые детей, с которыми они не встречались в реальной жизни.

Взрослым следует помнить, что общение детей по сети Интернет не должно быть бесконтрольным, иначе это может привести к

- киберзависимости,
- заражению вредоносными программами при скачивании файлов,
- нарушению нормального развития ребенка,
- неправильному формированию нравственных ценностей,
- знакомству с человеком с недобрыми намерениями.

Последние два пункта в особенности определяются анонимностью общения в Интернете, способствующих быстрому возникновению доверительных и дружеских отношений. Преступники используют преимущества этой анонимности для завязывания отношений с неопытными молодыми людьми. Взрослые смогут защитить детей, если будут в курсе того, чем они занимаются в Сети Интернет.

Преступники преимущественно устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой на конференции. Злоумышленники часто сами там обитают. Они стараются привлечь подростка своим вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей. Некоторые преступники могут действовать быстрее других и сразу же заводить сексуальные беседы. Преступники могут также предложить встречу с детьми в реальной жизни. Поэтому существует ряд общих правил, выполнение которых в значительной мере позволит обезопасить детей и подростков при работе в Интернете:

- ребенку не следует давать частной информации о себе (фамилию, номер телефона, адрес, номер школы) без разрешения родителей;
- не следует открывать письма электронной почты, файлы или Web-страницы, полученные от людей, которые не знакомы или не внушают доверия;
- ребенку не следует давать свой пароль кому-либо, за исключением взрослых членов семьи;
- следует объяснить ребенку, что он не должен делать того, что может стоить семье денег, кроме случаев, когда рядом с ним находятся родители;
- встреча в реальной жизни со знакомыми по Интернет-общению не является очень хорошей идеей, поскольку люди могут быть разными в электронном общении и при реальной встрече, и, если ребенок желает

встретиться с ними, родителям следует пойти на первую встречу вместе с ним.

Большинство детей, преследуемых Интернет-преступниками, проводят большое количество времени в Сети, особенно в чатах. Подчас закрывают дверь в свою комнату и скрывают, чем они занимаются, сидя за компьютером. Если в семейном компьютере появились материалы откровенного содержания, это повод для беспокойства. В качестве предлога для начала сексуальных обсуждений злоумышленники могут снабжать детей фотографиями, ссылками на соответствующие сайты и присылать сообщения эротической окраски. Для того чтобы внушить ребенку мысль о естественности сексуальных отношений между взрослыми и детьми, преступники могут использовать фотографии с изображением детской порнографии. Следует иметь в виду, что ребенок может прятать порнографические файлы на дисках, особенно если другие члены семьи пользуются тем же компьютером.

Установив в Интернете контакт с ребенком, некоторые злоумышленники могут попытаться вовлечь детей в секс по телефону или попытаться встретиться в реальной жизни. Если дети не решаются дать номер телефона, злоумышленник может сообщить им свой. Не разрешайте ребенку лично встречаться с незнакомцем без контроля со стороны родителей.

Преследователи могут посылать своим потенциальным жертвам письма, фотографии и подарки. В ряде стран они порой даже отправляют билеты на самолет, чтобы соблазнить ребенка личной встречей. Если ребенок начал сторониться семьи и друзей, быстро выключает монитор компьютера или переключается на другое окно, если в комнату входит взрослый, можно говорить о том, что он стал жертвой преступника. Интернет-преступники усердно вбивают клин между детьми и их семьями и часто преувеличивают небольшие неприятности в отношениях ребенка с близкими. Кроме того, дети, подвергающиеся сексуальному преследованию, становятся замкнутыми и подавленными.

Использование чужой учетной записи для выхода в Интернет также может свидетельствовать о нападении преступника. Даже при условии, что дети не имеют доступа в Сеть дома, могут встретить преследователя, выйдя в Интернет у друзей или в каком-нибудь общественном месте, например библиотеке. Иногда преступники предоставляют своим жертвам учетную записи, чтобы иметь возможность с ними общаться.

Что делать, если ребенок стал потенциальной целью преступника?

Регулярно проверяйте компьютер на наличие материалов откровенного характера или каких-либо свидетельств об общении с сексуальной окраской – этостораживающие признаки. Контролируйте доступ вашего ребенка ко всем средствам общения, работающим в режиме реального времени, таким, как чаты, мгновенные сообщения и электронная почта. Обычно Интернет-преступники впервые встречают своих потенциальных жертв в чатах, а затем

продолжают общаться с ними посредством электронной почты или мгновенных сообщений.

Не вините детей. Если, несмотря на все меры предосторожности, дети познакомились в Интернете со злоумышленником, вся полнота ответственности всегда лежит на правонарушителе. Предпримите решительные действия для прекращения дальнейших контактов ребенка с этим лицом.

Если ребенок получает фотографии откровенного характера или подвергается сексуальным домогательствам, сохраните всю имеющуюся информацию, включая адреса электронной почты, адреса сайтов и чатов, чтобы иметь возможность ознакомить с ней представителей власти.

Устойчивое понимание того, что проблема детской безопасности в Интернете — это предмет, требующий скоординированного решения на всех уровнях от семейного и муниципального до регионального и международного, в мире уже существует. В решении этой проблемы необходимо действовать системно и использовать не только правовые регуляторы, но и нормы обычаев и морали, а также технические и технологические возможности. Новым и самым эффективным механизмом решения этой проблемы может и должно стать формирование информационной культуры личности родителей и детей, а также профессиональной информационной культуры учителей.

Необходимо с первого знакомства с информационными технологиями разъяснять ребенку, как ему жить в информационном пространстве, как избирательно подходить к информации в открытой информационной среде. Важно, чтобы и сами родители, и дети понимали, что в информационном пространстве есть свои плюсы и минусы, плохое и хорошее.

Дети всегда думают, что они контролируют ситуацию. Они, хотя и слышали разговоры о случаях преследования незнакомцами людей, в результате которых кто-то пострадал от кражи личных данных или проникновения в компьютер, но по наивности думают, что с ними такое не случится, и они защищены от таких несчастных случаев.

В реальном мире дети руководствуются принципами, которые они выучили в школе и дома, но в виртуальном мире об этих принципах забывают. Они не понимают, что одни и те же средства самозащиты следует применять как в реальном, так и в виртуальном мире. Вот почему так важно научить детей тому, как безопасно общаться в Интернете.

Вопросы:

1. О каких правилах следует помнить ребенку, чтобы не стать потенциальной жертвой преступника?
2. Как узнать, стал ли ребенок потенциальной целью преступника?
3. Что делать, если дети подвергаются запугиванию в Интернете?

Тема 2. Безопасное общение детей в Интернете.

Цель: формирование представлений об Интернет-этике как одной из основ безопасного общения.

План лекции:

1. Интернет-этика. Основы поведения пользователей в сети Интернет.
2. Безопасное общение детей в Интернете. Правила безопасности в Интернете для детей разного возраста.
3. Основы безопасного ведения Интернет-дневников.
4. Безопасное общение с использованием веб-узлов социальных сетей.
5. Безопасное общение в чатах.
6. Безопасность участия детей в on-line играх.

Специального **"сетевого этикета"**, конечно же, не существует. Этикет всегда и везде один, что на улице, что в трамвае, что в Интернете. Хорошо воспитанный человек всегда и везде ведет себя прилично вне зависимости от того, о каком конкретно месте идет речь. Поэтому манеры поведения в Интернете ничем не отличаются от манер поведения в реальной жизни. Но именно анонимность пользователей сети Интернет способствует росту пренебрежения к подобным правилам, и иногда за клавиатурой компьютера люди делают такие вещи, которые никогда не сделали бы в реальной жизни.

Следует объяснить детям, что их могут выследить, что в Сети нет ничего анонимного. Все, сказанное в Интернете, должно быть сказано с пониманием того, что другие рано или поздно прочитают и узнают об этом.

Если Вы хотите, чтобы дети стали ответственными пользователями, объясните им **фундаментальные правила поведения в Сети:**

- *прежде, чем что-нибудь сказать или сделать, следует узнать правила общения на сайте.* Некоторые чаты и форумы имеют специальные правила, поясняющие, что имеет право говорить и делать пользователь. Поскольку многие люди критически относятся к тем, кто нарушает правила, знание правил может избавить ребенка от ненужного дискомфорта.
- *при общении на форуме не стоит отклоняться от темы разговора и следует ожидать своей очереди для ответ.*
- *думайте прежде, чем что-либо напечатать.* Удостоверьтесь, что Вы пишете приемлемые вещи, которые не приведут к конфликту. Единственное, в чем Вы можете не сомневаться – это в том, что все, сказанное Вами в Интернете, может вернуться и неотступно преследовать Вас.
- *не обращайтесь к другим пользователям в чате по их настоящему имени.*
- *не размещайте ложную информацию или грубые высказывания о другом человеке на форуме или в чате.*
- *не печатайте текст заглавными буквами.* Это может рассматриваться как крик, провоцирующий спор или конфликт.

- *не относитесь критически к другим, особенно к новичкам, даже если они нарушают правила.* Если существует необходимость помочь кому-то или исправить кого-то, следует сделать это по электронной почте, а не на общественном форуме (например, в чате). Не следует забывать, что все когда-то были новичками.
- *постарайтесь не тратить время других пользователей впустую:* не посылайте цепочку электронных писем, не передавайте киберслухи, не разыгрывайте других, не рассылайте спам.
- *не отправляйте большие вложенные файлы, не спросив разрешения у получателя.*
- *защищайте личную жизнь и личную информацию других пользователей:* не публикуйте в on-line чей-либо адрес электронной почты без разрешения владельца (вместо этого можно использовать опцию «Отправить по электронной почте»), не используйте без разрешения чужой пароль.
- *Не присваивайте условно-бесплатного программного обеспечения, не платя за него.*



Ребенок должен четко уяснить и запомнить: тот факт, что он скрывается за монитором компьютера, не освобождает его от корректного и вдумчивого общения!

Прежде чем начать собственное исследование киберпросторов ребенок должен некоторое время поработать под присмотром старших: родителей или преподавателей, и следовать правилам безопасной работы детей в сети Интернет учитывая при этом их возрастные особенности.

Советы по безопасности в Интернете для детей до 10 лет



Для детей в возрасте от 2 до 10 лет Интернет — это отличное место, где они могут играть и учиться.

1. **Налаживайте открытое и дружественное общение с детьми, говорите с ними о компьютерах и не игнорируйте их вопросы и любопытство.**
2. **Когда дети этого возраста пользуются Интернетом, родители всегда должны быть рядом с ними.**
3. **Составьте четкие правила использования Интернета.**
4. **Настаивайте на том, чтобы дети не раскрывали личные сведения, например: свое настоящее имя, адрес, номер телефона или пароли, - людям, с которыми они познакомились в Интернете.**
5. **Помогите детям придумать псевдонимы, не раскрывающие никаких личных сведений, если на веб-узле будет запрошено имя для персонализации отображаемых материалов.**
6. **Ознакомьтесь со средствами фильтрации веб-содержимого (например, функция родительского контроля в Windows), которые помогут найти общий язык с детьми и установить родительский контроль.**

7. При использовании средств обеспечения безопасности для всей семьи, создайте профили для каждого члена семьи в зависимости от его возраста.

8. Защитите детей от назойливых всплывающих окон с помощью функции блокирования всплывающих окон в обозревателе Internet Explorer.

9. Все члены семьи должны показывать пример поведения детям, которые только начинают использовать Интернет.

Советы по безопасности в Интернете для детей 11–14 лет

Дети этого возраста обычно очень восприимчивы они обладают хорошими способностями к выполнению компьютерных команд, использованию мыши и компьютерным играм. Однако при восприятии сведений из Интернета они во многом зависят от взрослых или старших братьев и сестер. Родителям, имеющим детей такого возраста, следует контролировать использование компьютера и применять специальные средства, такие как служба семейной безопасности Windows Live OneCare или функция родительского контроля в Windows Vista.

1. Поддерживайте открытые, дружеские отношения с детьми. Говорите с ними о компьютерах и не игнорируйте их вопросы и любопытство.

2. Составьте четкие правила использования Интернета.

3. Настаивайте на том, чтобы дети не раскрывали личные сведения.

4. Помогите детям придумать псевдонимы, не раскрывающие никаких личных сведений, если на веб-узле будет запрошено имя для персонализации отображаемых материалов.

5. Создайте профили для каждого члена семьи с помощью средств обеспечения безопасности для всей семьи.

6. Установите средний уровень для параметров безопасности средства обеспечения безопасности семьи, что позволит применить некоторые ограничения к содержимому посещаемых веб-узлов и действиям пользователей.

7. Установите компьютеры с подключением к Интернету в общих комнатах, где легко наблюдать за детьми.

8. В качестве дополнения к родительскому контролю используйте средства фильтрации веб-содержимого (например службу семейной безопасности Windows Live OneCare (EN)).

9. Защитите детей от назойливых всплывающих окон с помощью функции блокирования всплывающих окон в обозревателе Internet Explorer.

Для блокирования всплывающих окон в автономном режиме можно использовать Защитник Windows. Защитник Windows входит в состав системы Windows Vista. Для системы Windows XP с пакетом обновления 2 (SP2) Защитник Windows можно загрузить бесплатно.

10. Попросите детей сообщать вам, если что-то или кто-то в Интернете угрожает им или доставляет неудобства. Ведите себя спокойно и напоминайте детям, что они могут без опасений рассказывать вам обо всем.

Поощряйте их за правильное поведение и просите обращаться к вам снова в подобных ситуациях.

Советы по безопасности в Интернете для детей от 15 до 18 лет



Подростки должны иметь практически неограниченный доступ к содержимому, веб-узлам или деятельности в Интернете. Несмотря на то, что подростки лучше разбираются в Интернете, родители все же должны снабдить их соответствующими рекомендациями по обеспечению безопасности. Они должны быть готовы помочь детям и объяснить, как распознавать неприемлемые сообщения и избегать небезопасные ситуации. Может потребоваться напомнить детям о недопустимости передачи личных сведений через Интернет. Юноши этого возраста обычно интересуются юмором, играми или другими веб-узлами с мультимедийным содержанием. Девушки более склонны к созданию социальных сетей и участию в них.

1. Продолжайте поддерживать открытое и дружественное общение с детьми на тему компьютеров. Обсуждайте с ними их действия в Интернете и найденных там друзей так, будто речь идет о событиях и друзьях из реальной жизни.

2. Установите компьютеры с подключением к Интернету в общих комнатах, а не в комнатах детей.

3. В качестве дополнения к родительскому контролю используйте средства фильтрации веб-содержимого (например функцию родительского контроля в Windows Vista (EN) или службу семейной безопасности Windows Live OneCare (EN)).

4. Защитите детей от назойливых всплывающих окон с помощью функции блокирования всплывающих окон в обозревателе Internet Explorer. Для блокирования всплывающих окон в автономном режиме можно использовать Защитник Windows. Защитник Windows входит в состав системы Windows Vista. Для системы Windows XP с пакетом обновления 2 (SP2) Защитник Windows можно загрузить бесплатно.

5. Узнавайте у детей, какие чаты и доски объявлений они посещают и с кем общаются. Поощряйте общение в отслеживаемых комнатах бесед (чатах) и настаивайте на том, чтобы дети общались только в общих окнах комнат бесед.

6. Не разрешайте детям встречаться с друзьями из Интернета.

7. Объясните детям, что они не должны загружать из Интернета программы, музыку или файлы без вашего разрешения. Обмениваясь файлами и загружая из Интернета текст, изображения и другие материалы, они могут нарушить законы об авторских правах.

8. Расскажите детям о порнографии и других материалах для взрослых в Интернете и направьте их на веб-узлы с грамотными материалами о здоровье и половой жизни.

9. Помогите своим детям защититься от нежелательной почты. Научите их не сообщать в Интернете свои адреса электронной почты, не

отвечать на нежелательную почту и пользоваться фильтрами электронной почты.

10. Расскажите детям об ответственном и порядочном поведении в Интернете. Они не должны использовать Интернет для хулиганства, распространения слухов или угроз.

11. Проследите за тем, чтобы дети советовались с вами перед заказом, покупкой или продажей чего-либо в Интернете.

12. Обсудите с детьми азартные игры в Интернете и связанный с ними риск. Напоминайте им, что играть в азартные игры в Интернете запрещено законом.

Интернет предоставляет несколько форм общения, которые любят использовать дети и подростки: чаты, системы обмена мгновенными сообщениями, *блоги или Интернет-дневники*.

Увлечение веб-журналами (или, иначе говоря, блогами) распространяется со скоростью пожара, особенно среди подростков. Правильное ведение дневника дает:

- новые возможности общения с друзьями и родственниками,
- привитие ответственности и дисциплины ведения дневника,
- возможность творческого самовыражения,
- обучение компьютерным и Интернет-технологиям,
- развитие навыков набора на клавиатуре, правописания, письменной речи и редактирования.

Современная действительность такова, что примерно половина всех веб-журналов принадлежат подросткам. И, как показывают последние исследования, двое из трех раскрывают свой возраст, трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Не секрет, что подробное раскрытие личных данных потенциально опасно.

При этом все больше молодых пользователей создают собственные дневники, и каждый стремится привлечь как можно большее внимание аудитории. Иногда это приводит к тому, что дети размещают в блогах такой неуместный материал, как провокационные фотографии свои или друзей.

Поэтому с целью обеспечения безопасного общения детей в Интернет взрослым следует:

- установить для детей правила работы в Интернете;
- на первых порах следует просматривать то, что дети планируют отправить, так как по сведениям, которые могут казаться безобидными, например символу школы или фотографии города, можно определить, какую школу посещает автор;
- разъяснить детям, что никогда не следует публиковать в дневниках какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения;

никогда не помещать в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверять, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию;

– оцените качество работы службы веб-журналов и выясните, предлагает ли она личные, защищенные паролем веб-журналы;

Родителям рекомендуется хранить веб-адрес блога ребенка и регулярно его просматривать. Кроме того, следует рекомендовать детям, во-первых, пользоваться веб-журналами только с ясно сформулированными условиями использования и проверять, можно ли защитить с помощью пароля сами веб-журналы, а не только учетные записи пользователя. Но даже если это так, лучше секретную информацию держать в уме, потому что любой человек может получить доступ к Интернет-дневнику. Во-вторых, дети должны знать, что публикуемая в Интернете информация остается там надолго, и кто угодно может легко распечатать веб-журнал или сохранить его на своем компьютере.

Социальные веб-узлы также крайне популярны у подростков и набирают все большую популярность среди детей младшего возраста. Дети используют веб-узлы социальных сетей для общения как с детьми из других частей мира, так и с теми, кого каждый день встречают в школе. Причем, посещать могут как социальные веб-узлы, созданные специально для детей (например, Webkinz или Club Penguin), так и веб-узлы, предназначенные для взрослых (например, Windows Live Spaces, YouTube, MySpace, Flickr, Twitter, Facebook и другие).

На веб-узлах социальных сетей дети выражают свои чувства, а иногда даже ищут сведения о ком-то, кого им довелось повстречать на вечеринке или в школе. Например, после личной встречи ребенок может посетить веб-узел своего нового знакомого, чтобы лучше понять, хочет ли он с ним подружиться.

На эти веб-узлах дети

- общаются;
- играют в игры;
- размещают свои фотографии и видеоролики и смотрят чужие;
- ведут блоги;
- публикуют данные о себе.

Однако, что бы дети ни делали, они должны понимать, что многие такие веб-страницы может увидеть любой человек, имеющий доступ в Интернет. К сожалению, некоторые сведения, размещаемые детьми на своих страницах, могут сделать их объектом **фишинг-афер**, запугивания и действий Интернет-преступников.

Существуют несколько способов, позволяющих сделать использование веб-узлов социальных сетей более безопасным для ребенка:

- *Взрослым следует обсудить с детьми их опыт использования веб-узлов.* Попросите детей рассказывать вам о том, что их пугает при общении на веб-узлах, или вызывает дискомфорт. Ведите себя спокойно и

напоминайте детям, что они могут без опасений рассказывать вам обо всем. Объясните, что готовы помочь им разрешить любую ситуацию благоприятным образом.

– *Установите правила пользования Интернетом дома.* По мере того как дети начинают самостоятельно пользоваться Интернетом, имеет смысл составить список правил его использования, который бы их устроил. В этих правилах должно быть указано, разрешается ли ребенку посещать веб-узлы социальных сетей и на каких условиях. Для каждого ребенка можно составить отдельный договор с правилами пользования Интернетом, установленными в соответствии с его возрастом. Пример договора (приложение №1).

– *Убедитесь, что дети следуют ограничениям по возрасту, установленным на веб-узле.* Рекомендуемый возраст регистрации на веб-узлах социальных сетей — 13 лет и старше. Если дети младше рекомендуемого возраста, не позволяйте им посещать эти веб-узлы. Помните, что сами службы могут не препятствовать регистрации малолетних детей.

– *Изучите веб-узел сами.* Просмотрите сайты, которые собирается посещать ребенок, и убедитесь, что и вы, и ребенок понимаете суть политики конфиденциальности и кодекса поведения. Выясните, отслеживается ли на сайте размещаемое его пользователями содержимое. Кроме того, периодически просматривайте страницу своего ребенка.

– *Запретите детям лично встречаться с теми, с кем они общались исключительно в Сети, убедите их общаться только с людьми, которых они знают лично.* Дети могут подвергнуться серьезной опасности при личной встрече с людьми, с которыми они общались исключительно в Интернете. Чтобы защитить своих детей от этой опасности, убедите их использовать такие веб-узлы для общения только со своими друзьями, а не с незнакомыми людьми. Учтите, что может оказаться недостаточным просто запретить ребенку общаться с незнакомыми людьми, потому что он может не считать незнакомым человека, с которым «познакомился» в Сети.

– *Убедитесь в том, что дети не используют полные имена.* Пусть ребенок использует только имя или псевдоним, который не будет привлекать излишнего внимания. Также запретите детям использовать полные имена своих друзей.

– *Контролируйте размещение любых других личных данных в профиле ребенка.* Многие веб-узлы социальных сетей позволяют детям входить в общие группы, которые объединяют учащихся одной школы. Внимательно относитесь к ситуациям, когда дети размещают сведения о себе, с помощью которых можно выяснить их личность (например, эмблему своей школы, фотографию рабочего места или название города, в котором они живут). Излишняя открытость может сделать ребенка объектом запугивания, мошенничества, действий Интернет-преступников или кражи личных сведений.

– *Обращайте внимание на детали фотографий.* Объясните ребенку, что по фотографиям можно многое узнать о человеке. Убедите детей не размещать свои фотографии или фотографии друзей с легко узнаваемыми деталями, такими как названия улиц, номера машин или название школы на одежде.

– *Рассмотрите возможность использования веб-узла с ограничением доступа.* Некоторые веб-узлы социальных сетей позволяют защищать свою страницу с помощью пароля или реализуют другие методы защиты, разрешая просмотр сведений о детях только тем, кого они знают. Например, служба MSN Spaces позволяет указать, кому разрешается просматривать веб-узел, начиная от всех пользователей Интернета и заканчивая только выбранными людьми.

– *Предупредите ребенка, что нельзя выставлять на показ свои чувства незнакомым людям.* Дети используют веб-узлы социальных сетей, чтобы вести дневники и писать стихотворения, в которых часто весьма открыто выражают свои чувства. Объясните детям, что их записи может прочитать кто угодно, у кого есть доступ к Интернету, и что Интернет-преступники охотятся на эмоционально ранимых детей.

– *Расскажите детям о запугивании через Интернет.* Как только дети достаточно повзрослеют для посещения веб-узлов социальных сетей, расскажите им о практике запугивания в Интернете. Объясните ребенку, что если ему кажется, что его запугивают, следует сказать об этом родителям, учителю или кому-то из взрослых, кому он доверяет. Кроме того, нужно пояснить ребенку, что общаться с другими людьми в Интернете надо так же, как он общался бы с ними вживую.

– *Удаление страницы ребенка.* Если ребенок отказывается подчиняться установленным вами правилам, призванным его защитить, то после попытки на него повлиять можно связаться с администрацией веб-узла социальной сети, которую посещает ребенок, и попросить удалить его страницу.

Существуют способы, с помощью которых можно отследить, какие веб-узлы посещал ребенок. Но следует иметь в виду, что дети, которые хорошо разбираются в компьютерах, умеют скрывать свои действия в Интернете. Поэтому эффективнее иметь четкие правила работы в Интернете и открыто общаться с детьми. Кроме того, многие виды программного обеспечения позволяют контролировать действия в Интернете. Например, родительский контроль в Windows Vista позволяет фильтровать содержимое Интернета. Эти программные средства еженедельно отправляют вам отчеты об активности, в которых содержатся подробные сведения о веб-узлах, которые посещали ваши дети, людях, с которыми они общались и т. д.

Интернет предоставляет пользователям ряд возможностей, в том числе общаться с другими людьми в режиме реального времени. Причем, если раньше в **чатах** пользователи могли общаться только путем ввода сообщений с клавиатуры, современные средства позволяют вести голосовые

(необходимо наличие микрофона и колонок) и даже видеобеседы (потребуется Web-камера).

Для того чтобы начать беседу в Интернете, необходимо зайти в чат-знакомство. После входа в чат можно читать на экране сообщения других участников и добавлять свои собственные комментарии, просто вводя их с клавиатуры и щелкая по кнопке «Отправить». Если в беседе участвуют несколько человек, они могут вводить свои реплики одновременно. Все реплики появляются в окне и помечаются псевдонимами собеседников. В некоторых системах для ведения бесед каждый участник может выбрать свой тип шрифта и цвет.

На многих Web-узлах имеются комнаты для бесед, доступ к которым может получить каждый посетитель узла. Каждый, у кого есть доступ в Интернет, может воспользоваться старомодной системой под названием IRC Chat — посиделки в Интернете, которая остается достаточно популярной и в наше время, хотя пользоваться ею достаточно затруднительно.

Сущность сеансов бесед в целом не зависит от типа используемых систем. Каждая комната для бесед имеет свое название, которое обычно определяет тему беседы и по которому иногда можно судить о том, какого типа люди ее ведут.

Независимо от того, какая система используется для ведения бесед, каждый участник должен выбрать себе псевдоним (на сленге — ник), который был бы достаточно колоритным и одновременно служил маской истинного имени пользователя.

Ввиду тотальной анонимности сеансы бесед являются местом, где, с одной стороны, следует соблюдать особую осторожность поведения. С другой стороны, беседы ведутся для того, чтобы познакомиться с новыми интересными людьми. Много теплых и чудесных дружеских связей развилось из случайных встреч в комнатах для бесед. Когда вы подключаетесь к группе уже после начала беседы, на экране отображены псевдонимы людей, которые участвуют в беседе, и окно текущего разговора. Если группа дружелюбная, то после вашего появления в группе кто-нибудь наверняка пошлет вам приветствие.

При знакомстве с новым человеком в интерактивной дискуссионной группе, возможно, захочется перейти от общения в общественном чате к более личной беседе с глазу на глаз. Например, можно начать беседу в общей комнате чата, а затем перейти к общению с помощью программы мгновенного обмена сообщениями или переписке по электронной почте. При использовании этих средств можно по-прежнему обеспечить защиту своей личности путем использования псевдонима (например, псевдоним01@домен.ru). Кроме того, такой тип адреса проще предоставить на случай, если новым контактом окажется человек, с которым необходимо будет прекратить общение.

Взрослым следует быть осторожными и не позволять детям принимать участие в подобных беседах без их наблюдения. Так как, несмотря на то, что существуют специально предназначенные комнаты для бесед детей, в

которых предпринимаются некоторые меры предосторожности с целью безопасного общения, в них все равно иногда проникают люди, общение с которыми может оказаться вредным для ребенка. Люди в комнатах для бесед часто говорят неправду о своих занятиях, возрасте, месте жительства и, увы, даже скрывают свой пол. Кто-то считает себя очень остроумным, кто-то фантазирует, а кто-то по-настоящему болен.

Дети, которые общаются в чатах, должны знать, как сделать такое общение безопасным:

- не доверять никому личную информацию: место жительства, почтовый адрес, фамилию или телефонный номер, адрес школы, которую посещает ребенок, личные сведения о членах своей семьи, даже если за заполнение подобной формы предложат какой-нибудь приз, и т. п.;
- сообщать администратору чата о проявлениях оскорбительного поведения участников;
- если ребенку неприятно находиться в чате, его следует покинуть;
- если ребенку что-то не понравилось, обязательно следует рассказать об этом родителям;
- детям рекомендуется отказываться от участия в личных интерактивных беседах с людьми, которых они не знают в жизни. Кроме того, если система для ведения бесед поддерживает создание профилей, а кто-то, не имеющий профиля, желает с ребенком пообщаться, следует быть вдвойне осторожным.
- не встречаться без ведома и согласия родителей с человеком, с которым познакомились в on-line режиме.

Взрослые могут судить о степени безопасности чата, в котором общается ребенок, ответив утвердительно на три основных вопроса:

1. Предназначен ли чат для детей?

В чатах, предназначенных для детей, вероятность неуместных тем или нежелательного контакта гораздо ниже.

2. Осуществляется ли контроль за чатом?

Иногда в чатах работают добровольные модераторы, которые предотвращают случаи неуместного общения и могут заблокировать доступ в чат для хулиганов и других нарушителей порядка. Если контроль не осуществляется, в чате, по крайней мере, должна иметься кнопка для связи с администратором. Для детей предпочтительны контролируемые чаты. Уровень безопасности также повышается, если беседы сохраняются.

3. Возможно ли заблокировать доступ для пользователей?

Блокировка доступа подразумевает запрет размещения в чате сообщений от конкретного пользователя. После блокировки доступа для пользователя его сообщения больше не отображаются на экране.

Безопасность при on-line играх. Так же, как и в обычной жизни, в Интернете появились свои хулиганы, которые осложняют жизнь другим пользователям Сети. Их называют *гриферами*. Есть вероятность, что один из таких злодеев по крайней мере единожды побеспокоит ребенка в таких многопользовательских играх, как Halo 2, EverQuest, The Sims Online,

SOCOM и Star Wars Galaxies. Гриферы получают удовольствие, хамя и грубя окружающим. Обычно они издеваются над другими, особенно над начинающими: мешают играть товарищам по команде, используют нецензурную лексику, жульничают, создают вместе с другими гриферами бродячие банды, блокируют выходы из комнат, выманивают монстров на неосторожных игроков или используют игру, чтобы досадить кому-то или изводить конкретного человека.

Хотя гриферы составляют лишь малую часть от общего числа пользователей, из-за них некоторые компании потеряли клиентов. Поэтому многие разработчики игр не жалеют средств и используют любые методы для вычисления гриферов.

Как поступать, если дети столкнулись с гриферами?

Пусть дети их игнорируют. Если ребенок не будет реагировать на воздействия гриферов, большинству из них это в конце концов надоедает, и они уходят.

Посоветуйте детям изменить параметры игры. Добейтесь, чтобы ребенок играл в игры, правила или режимы которых можно изменить (например, невозможность убить товарищей по команде). Таким образом, тактика гриферов становится бессмысленной.

Рекомендуйте создать частную игру. Большинство многопользовательских игр позволяет создавать закрытые комнаты, куда можно пускать только друзей.

Пусть дети играют на сайтах со строгими правилами. Там, где установлены строгие правила, тогда администратор сможет немедленно заблокировать хулиганов.

Пусть играют в игры, где от гриферов можно легко избавиться: сообщения хулиганов можно отключить или проголосовать за их исключение из игры.

Поищите вместе с ребенком уязвимости в игре или новые способы жульничества. Сообщайте о своих находках администратору.

Если обидчик продолжает беспокоить ребенка, добейтесь, чтобы он сменил игру или сделал перерыв и вернулся позже.

Пусть ваши дети воздерживаются отвечать огнем на огонь. Убедитесь, что ребенок не использует против обидчиков их же тактику: скорее всего, это спровоцирует гриферов на еще более озлобленное поведение. Или, что еще хуже, создаст о ребенке впечатление как об обидчике.

Вопросы:

1. Что подразумевается под понятием «сетевой этикет»?
2. Какие правила поведения в сети Вам известны?
3. Сформулируйте правила общения в чатах.
4. Кто такие «гриферы»? Как помочь ребенку, посещающему сайты многопользовательских игр, столкнувшемуся гриферами?

5. В каком возрасте целесообразнее знакомить детей с правилами поведения в сети Интернет?
6. Каковы основы безопасного общения в блогах?
7. Перечислите способы, позволяющие сделать использование веб-узлов социальных сетей безопасным для ребенка.
8. Какими должны быть «внутренние правила» использования Интернета?
9. Может ли взрослый отследить, какие веб-узлы посещают дети? Каким образом?

Тема 3. Феномен «Интернет-зависимости». Профилактика Интернет-зависимости.

Цель: формирование представлений феномене «Интернет-зависимости», о причинах возникновения и методах профилактики с интернет-зависимостью.

План лекции:

1. Феномен «Интернет-зависимости».
2. Причины возникновения Интернет-зависимости.
3. Основные типы Интернет-зависимости.
4. Профилактика Интернет-зависимости.

Информация для человека имеет огромное значение. Компьютер и Интернет является мощным инструментом обработки и обмена информацией, кроме того, благодаря компьютеру стали доступными различные виды информации. Это и считается первопричиной компьютерной или *Интернет зависимости*, так как в определенном смысле они страдают нарушением процессов обмена информацией.

Проблема Интернет-зависимости выявилась с возрастанием популярности сети Интернет. Некоторые люди стали настолько увлекаться виртуальным пространством, что начали предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Резкий отказ от Интернета вызывает у таких людей тревогу и эмоциональное возбуждение. Многие люди считают Интернет-зависимость сходной с химической зависимостью вроде курения или наркомании. Психиатры же усматривают схожесть такой зависимости с чрезмерным увлечением азартными играми. Разумеется, возможны как положительные, так и отрицательные психологические последствия появления Интернет для образовательной среды в школе.

Рассмотрим особенности Интернета, которые могут вызывать полярные психологические последствия.

1. Интернет обширен. Интернет - это среда, в которой нет границ (национальных, социальных, географических). Учащийся, находясь в контакте с такой средой, сталкивается с разнообразнейшими фактами и мнениями, о существовании которых он мог и не подозревать; он знакомится со сверстниками за рубежом и в других городах, имеет возможность задать вопросы и с несравнимой с другими способами получения информации скоростью добыть ответ на совершенно различные интересующие его темы, не вставая с места, например: а как там учатся, кто и где? Это позволяет учащимся ощущать себя причастными к какому-либо сообществу, развивает способность к децентрации.

2. Интернет безопасен. Общение не несет в себе агрессивного невербального компонента, а вербальных оскорблений гораздо меньше. Они конечно же присутствуют, но на многих сайтах с этим успешно справляются. Это удовлетворяет базовую потребность в безопасности.

3. В Интернет нет централизованной цензуры: можно написать то, что хочется, высказать свое мнение. Это позволяет чувствовать себя раскованным в общении, интересным для других, компетентным. Ребенок или взрослый всегда может найти тот круг общения, в котором он будет выглядеть именно так. Это удовлетворяет потребность в принятии, дружеском расположении, позволяет безопасно выражать свою индивидуальность.

4. Интернет безличен. Человек может обладать множественной идентичностью, превращая в миф ранее неизменное выражение: «Одна личность - одно тело» (и соответственно пол). За счет этого качества может происходить компенсация деструктивных наклонностей личности, поскольку есть возможность отыграть сценарий, который невозможно реализовать в жизни.

5. Интернет как фактор дополнительной мотивации. Поиск и нахождение информации, подчас уникальной, позволяет ученику углубляться в предмет, что делает его привлекательнее. Часто возникает "эффект потока", когда поиск информации превращается в самоцель. Вызывает трансное состояние.

6. Интернет прост. Его использование доступно для детей младших классов.

7. Интернет современен и доступен. Обучение информационным технологиям, постоянное повышение качества обслуживания и простота доступа увеличивают возможности учащегося занять достойное место в современном мире. То есть быть уверенным в себе.

Несмотря на все разнообразие активности пользователей Интернета, можно выделить **три основных вида, осуществляемой ими деятельности**: познавательную, игровую и коммуникативную. Этим разновидностям деятельности соответствуют глобальные изменения (трансформации) личности, которые в последнее время привлекли внимание широкой публики (конечно как однозначно негативные трансформации) и, в меньшей степени, исследователей:

1. Увлеченность познанием в сфере программирования и телекоммуникаций. Крайний вариант - хакерство.

2. Увлеченность компьютерными играми, в частности играми посредством Интернета. Крайний вариант - игромания.

3. Увлеченность сетевой коммуникацией. Крайний вариант - **Интернет-аддикция**.

Впервые расстройство было описано в 1995 году доктором Иваном Голдбергом, выделивший следующие основные симптомы этого расстройства:

– использование Интернета вызывает болезненное негативное стрессовое состояние или дистресс;

– использование Интернета причиняет ущерб физическому, психологическому, межличностному, экономическому или социальному статусу.

Интернет-зависимость определяется психологами как "навязчивое желание выйти в Интернет, находясь off-line, и неспособность выйти из Интернет, будучи on-line. Под on-line понимается общение в сети в реальном времени, off-line - общение через почтовый ящик, когда непосредственный собеседник отсутствует в данный момент времени. Исследователи приводят различные критерии, по которым можно судить об Интернет - зависимости.

Так, Кимберли Янг приводит четыре признака:

- навязчивое желание проверить e-mail;
- постоянное желание следующего выхода в Интернет;
- жалобы окружающих на то, что человек проводит слишком много времени в Интернет;
- жалобы окружающих на то, что человек тратит слишком много денег на Интернет.

Более развернутую систему критериев приводит Иван Голдберг. По его мнению, можно констатировать Интернет - зависимость при наличии 3-х пунктов из следующих:

- количество времени, которое нужно провести в Интернет, чтобы достичь удовлетворения (иногда чувство удовольствия от общения в сети граничит с эйфорией), заметно возрастает;
- если человек не увеличивает количество времени, которое он проводит в Интернет, то эффект заметно снижается;
- пользователь совершает попытки отказаться от Интернет или хотя бы меньше проводить в нем меньше времени;
- прекращение или сокращение времени, проводимого в Интернет приводит пользователя к плохому самочувствию, которое развивается в течении от нескольких дней до месяца и выражается двумя или более факторами: (эмоциональное и двигательное возбуждение, тревога, навязчивые размышления о том, что сейчас происходит в Интернет, фантазии и мечты об Интернет, произвольные или непроизвольные движения пальцами, напоминающие печатание на клавиатуре).

Первый и второй пункты отражают возникновение такого феномена, как толерантность. Похожие признаки можно наблюдать у курящих людей, алкоголиков и наркоманов, когда для получения удовольствия необходимо постоянно увеличивать дозировку. В данном случае «дозировкой» является количество времени затраченного на пребывание в виртуальном мире.

Преимущество Интернет - зависимости в отсутствии физиологического компонента. Синдром отмены вызывает у пользователя снижение или нарушение социальной, профессиональной или другой деятельности. В других исследованиях Интернет-зависимости было установлено, что Интернет-зависимые часто «предвкушают» свой выход в Интернет, чувствуют нервозность, находясь off-line, врут относительно времени

пребывания в Интернете, и чувствуют, что Интернет порождает проблемы на работе, финансовом статусе, а также социальные проблемы. К.Янг приводит данные других исследователей по которым студенты страдают от академической неуспеваемости и ухудшения отношений, и что это связано с неконтролируемым ими использованием Интернет.

Руководствуясь выше перечисленными характеристиками Интернет-зависимости, можно судить о собственной Интернет-зависимости или наличия таковой у своих знакомых. Психотерапевтический опыт показывает, что если человек признает у себя наличие того или иного вида зависимости, будь то зависимость от вредных веществ или от Интернета, то он пытается справиться с этим самостоятельно или с помощью близких ему людей, а также специалистов (психиатров, наркологов, психотерапевтов или психологов). Именно некритичное отношение к собственным проблемам, то есть отрицание их наличия, и делает из людей наркоманов, алкоголиков, Интернет-зависимых. Безусловно, по сравнению с зависимостями от вредных веществ Интернет-зависимость не так вредна, так как слабо проявляет себя на физическом уровне.

Заболеванию сопутствует подавленное настроение и депрессия, которые возникают в случае долгой отлучки от компьютера и сети. Депрессивное состояние при этом часто напоминает абстинентный синдром в слабой форме. В запущенных случаях зависимый перестает обращать внимание не только на окружающих, но и на себя, на свой внешний вид, перестает выполнять элементарные гигиенические процедуры: умываться, бриться и т. д. Доктор Янг разработала анкету, по которой можно самостоятельно провести диагностику интернет-зависимости. Русский вариант анкеты – на сайте www.psyhelp.ru/texts/iad_test.htm.

Задание 1. Определите с помощью анкеты доктора Янг зависимы ли Вы.

По мнению американских психологов, на формирование компьютерной зависимости уходит от полугода до года, в то время как другие формы привыкания формируются годами. По результатам опросов, проведенных российскими исследователями, зависимость от компьютера чаще встречается у тех, кто работает с этой техникой более пяти лет.

Причины возникновения Интернет-зависимости. Исследователи выяснили, что большая часть Интернет-зависимых пользуется сервисами, связанными с общением. Можно выделить две группы среди Интернет-зависимых: висящих на общении ради общения (91%) и висящих на информации.

В киберпространстве можно выражать свое мнение без страха отвержения, конфронтации или осуждения потому, что другие люди являются менее достигаемыми, и потому, что личность самого коммуникатора может быть замаскирована. Таким образом, благодаря общению в Интернете люди, склонные к созданию зависимостей, компенсируют свои потребности в общении и чувстве защищенности. Как наркотик, общение в Интернете

может создавать иллюзию благополучия, кажущуюся возможность решения реальных проблем. Хотя, как показывают исследования московских психологов, многие Интернет-зависимые отдают себе отчет в том, что не получают реальной поддержки в сети, и не расценивают Интернет как среду, гарантирующую общение. Известны алкоголики и наркоманы, которые сократили злоупотребление вредными веществами, а многие и вовсе отказались от них, благодаря многочасовым сессиям в Сети. То есть, они заместили одну зависимость на другую. В этом смысле Интернет-зависимость является более "экологичной". Итак, благодаря своим качествам: анонимности, доступности, невидимости, безопасности, простоты использования, Интернет оказывает неоценимую услугу людям, страдающим от вредных привычек, предоставляя им возможность отказаться от последних, и в то же время может наносить вред подросткам и молодежи, которые вместо социализации в реальном мире, находят возможность социализации в мире Виртуальном.

По данным различных исследований, Интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. Российские психиатры считают, что сейчас в нашей стране таковых 4—6 %. Несмотря на отсутствие официального признания проблемы, Интернет-зависимость уже принимается в расчёт во многих странах мира. Например, в Финляндии молодым людям с Интернет-зависимостью предоставляют отсрочку от армии.

Основные 5 типов Интернет-зависимостей таковы:

1. Навязчивый веб-серфинг – бесконечные путешествия по Всемирной паутине, поиск информации.

2. Пристрастие к виртуальному общению и виртуальным знакомствам — большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети.

3. Игровая зависимость – навязчивое увлечение компьютерными играми по сети.

4. Навязчивая финансовая потребность – игра по сети в азартные игры, ненужные покупки в Интернет-магазинах или постоянные участия в Интернет-аукционах.

5. Киберсексуальная зависимость – навязчивое влечение к посещению порносайтов и занятию киберсексом.

Статистика так распределяет сетевые услуги по частоте Интернет-зависимости:

1. Чаты — 37 %;
2. Многопользовательские игры — 28 %;
3. Телеконференции по сети — 15 %;
4. Электронная почта — 13 %;
5. Сайты Всемирной паутины — 7 %;
6. Иные сетевые протоколы (ftp, gopher и пр.) — 2 %.

Анализ показывает, что главенствующим фактором, благодаря которому все эти явления получили широкое распространение, является анонимность личности в Интернете.

Проблемы в семье, как правило, возникают в результате недостатка внимания к тому или иному члену семьи. Ссоры и непонимание проблем зависимого человека только усугубляют положения отношения в семье. Так как Интернет-зависимый человек поглощает много информации и возможно знаний, подобные изменения вызывают внутреннюю напряженность и обеспокоенность. Семейные скандалы могут лишь повредить человеку еще больше психику. Лучший способ решить проблемы семьи — это любовь, взаимопонимание и мудрость домочадцев. При этом необходимо плавно выводить человека на семейное позитивное общение и главное увеличивать совместное общение с живой природой, возможно это прогулки.

Психиатры и психологи отрицают, что в группу риска входят подростки, которые могут часами играть в компьютерные игры или общаться в чатах и форумах, и что у таких подростков могут в дальнейшем возникнуть проблемы с социальной адаптацией. По мнению Александра Майсова, информационная или любая другая зависимость от компьютера ничем не хуже патологической привязанности к чтению или, например, телевизору.

На сегодняшний день ни один психиатр или психотерапевт не может рекомендовать универсальный способ лечения от интернет- и компьютерной зависимости. Отмена или запрет может привести к усугублению ситуации, поскольку рождает чувство противоречия и стремление любой ценой обойти запрет. Только в том случае, если из-за одержимости компьютерами человек становится по-настоящему агрессивным, опасным для себя и окружающих, психиатры могут рекомендовать изолировать его на время от общества и лечить медикаментами. Самый простой и доступный способ решения зависимости - это приобретение другой зависимости. Любовь к здоровому образу жизни общение с живой природой, творческие прикладные увлечения, такие как рисование, как правило, выводят человека из зависимости.

Профилактика интернет-зависимости¹.

Проблема интернет-зависимости очень остро стоит во всем мире. Многие подростки и вполне зрелые люди проводят чудовищно много времени у экрана монитора. Люди начинают меньше спать и больше замыкаться в себе, что в результате приводит к нервным расстройствам, нарушениям сна, проблемам в работе и учебе и общении с друзьями. Бывали случаи, когда нездоровая тяга к информационным технологиям приводила к самоубийствам и убийствам.

Сегодня психиатры выделяют два метода лечения от интернет-зависимости: психофармакотерапия (прием психотропных средств) и

¹ По данным "Китайского национального детского центра" среди 18 миллионов несовершеннолетних китайцев, пользующихся интернетом, 13 процентов подвержено интернет-зависимости. В Китае насчитывается 113000 интернет-кафе. По предписанию "Национального народного конгресса", владельцы обязаны ограничивать несовершеннолетним китайцам доступ в кафе и время пользования компьютерами.

психотерапия (лечение без лекарств). Средняя продолжительность лечения от интернет-зависимости в России составляет около месяца. Однако, по словам врачей, официального диагноза "интернет-зависимость" пока в международной практике нет. Поэтому лечат, как правило, от проявлений привязанности к Сети.



Зависимость от интернета медики уже склонны считать серьезным заболеванием, которому подвержены миллионы людей во всем мире. Ученые отмечают, что зависимость от интернета - это опаснейшая угроза 21 века, которая выражается не только в психологических патологиях, таких как болезненное пристрастие к виртуальной жизни, но и в физических проявлениях. Одним из физических заболеваний является известный ортопедам синдром компьютерной мыши.

Самая большая угроза зависимости от интернета заключается в том, что это заболевание распространяется с колоссальной скоростью. Люди уже не просто играют, смотрят фильмы и слушают музыку в сети. В интернете они общаются, заводят романы, работают, отдыхают, делают покупки и путешествуют. При этом в реальности человек часто отходит от компьютера только чтобы поспать и поесть, и то не всегда. Реальная жизнь полностью заменяется виртуальной.

Существует "группа риска" среди учащихся, которые могут быть подвержены "интернет-зависимости". Они интровертированы, необщительны или не имеют коммуникативных навыков, умны. Их легко отличить по поведению: они погружены в себя, много фантазируют, держатся в стороне от одноклассников, иногда не успевают по предметам.

Итак, для профилактики зависимости от интернета необходимо:

- каждый час отвлекаться от монитора;
- больше читать;
- все свободное время стараться проводить вне помещения, в котором находится компьютер;
- для профилактики синдрома запястного канала и интернет-зависимости врачи советуют хотя бы раз в час разминать руки;
- учиться контролировать себя, а также не проводить попусту все свободное время перед экраном монитора.

Задание 2. Продолжите этот ряд профилактических мер, направленных против феномена «интернет-зависимость».

Вопросы:

1. Каковы основные признаки интернет-зависимости?
2. Какие действия необходимо предпринять, чтобы избавиться или снизить интернет-зависимость?
3. Какие выделяют основные типы интернет-зависимостей?

4. Какая категория учащихся в первую очередь попадает в зависимость от интернета?

Тема 4.1. Технология безопасной работы в сети

Цель: формирование представлений и навыков защиты детей и компьютера от опасностей Интернета с помощью программных средств.

Лекция 4. Четыре шага, которые помогут защитить компьютер от опасностей в Интернете.

Практическое занятие. Повышение уровня безопасности детей в Интернете при помощи программных средств: Центр обеспечения безопасности, Блокирование доступа к нежелательной информации, Блокирование спама, Создание отдельных учетных записей.

План:

1. Шаги, помогающие защитить компьютер от опасностей в Интернете.
2. Повышение уровня безопасности для операционной системы Microsoft®Windows® XP Service Pack 2.

Лекция 4. Четыре шага, которые помогут защитить компьютер от опасностей в Интернете

Интернет предоставляет детям доступ к играм и фильмам, а также бесконечные возможности для получения новых знаний и развития исследовательских навыков. Но эти преимущества сопровождаются и рядом сложных проблем. Утешает то, что можно предпринять некоторые шаги, которые помогут защитить детей от опасностей в Интернете. Только не стоит забывать, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются ваши дети за компьютером.

Далее представлены шаги, следуя которым можно защитить своих детей от вторжения в их личную жизнь и обеспечивают большую безопасность в Интернете. Итак,

- отобрать сайты, которые можно посещать;
- увеличить уровень защиты и конфиденциальности;
- следить за тем, какие сайты посещают дети;
- напоминать детям, основные правила общения в Интернете.

В первую очередь необходимо выяснить, что конкретно нужно родителю и ребенку в сети Интернет. Даже если есть полная уверенность в сайтах, на которые ходите, неплохо все же проверить страницы, сделанные

специально для детей. Особое внимание обратите на те серверы, что собирают личные данные посетителей.

В Интернете достаточно безопасных мест для детей. Если вы не хотите сообщать личные сведения о ребенке, поищите немного и, возможно, вы найдете аналогичный сайт, который не запрашивает абсолютно никаких личных данных.

Хотя программы и помогут защитить Вашу семью от нежелательной информации, ничто не заменит знания нескольких основных правил: расскажите своим детям об опасностях, существующих в Интернете, и научите правильно выходить из неприятных ситуаций; в заключение беседы установите определенные ограничения на использование Интернета и обсудите их с детьми. Сообща вы сможете создать для ребят уют и безопасность в Интернете.

Очень полезно составить список правил, которые ваши дети должны выполнять при каждом подключении к Интернету. Эти предписания можно даже повесить рядом с компьютером.

Три основных рекомендации

Внимание!!!

1. Никогда не сообщайте свое имя, номер телефона, адрес, пароль или номера кредитных карт.
2. Если вас что-то пугает в работе компьютера, немедленно выключите его.
3. Никогда не соглашайтесь на личную встречу с людьми, которых вы встретили в Интернете.

Блокирование доступа к неподходящим материалам

Один из наилучших способов защиты от нежелательной информации — это блокирование доступа еще до того, как она может быть получена.

1. С помощью панели обозревателя *Internet Explorer* 6. Панель *Microsoft Internet Explorer* 6 «Полезный совет» поможет ограничить доступ ребенка к информации в Сети. Можно задавать ограничения на основе собственных критериев, можно с помощью правил платформы отбора информационного содержимого PICS (*Platform for Internet Content Selection*) или системы рейтингов другой организации, вызывающей у вас доверие. Такие системы обычно предоставляют возможность выбора уровня конфиденциальности. Это позволит избежать ненормативной лексики, изображений обнаженных тел, сексуальных сцен, сцен насилия — при условии, что сайты, посещаемые вашим ребенком, присваивают каждой страничке точный рейтинг содержимого.

2. *Используя средства родительского контроля в MSN* 9. Программа *MSN* 9 также включает контроль над нежелательной информацией. В зависимости от возраста и развития ребенка можно выбрать

индивидуальный уровень защиты. Функции родительского контроля предоставляют полный список всех возможностей программы MSN 9.

3. *С помощью функций родительского контроля Xbox.* Они позволят ограничить доступ ребенка к неподходящим играм и DVD-фильмам.

Увеличение уровня защиты и конфиденциальности

Кроме блокирования нежелательной информации, полезно запретить доступ к сайтам, которые могут представлять опасность для вашей безопасности и конфиденциальности, рекомендуется следовать нижеприведенным правилам:

1. *Создайте отдельные учетные записи для разных пользователей.*


Windows XP позволяет создать несколько учетных записей. Каждый пользователь сможет входить в систему независимо и иметь уникальный профиль с собственным рабочим столом и папкой «Мои документы». Учитель (Родитель) может присвоить себе учетную запись администратора, дающую полный контроль над компьютером, а учащимся (детям) — ограниченные учетные записи. Такие пользователи не смогут изменить системные настройки или установить новое аппаратное или программное обеспечение, включая большинство игр, медиаплееров и программ поддержки чатов.

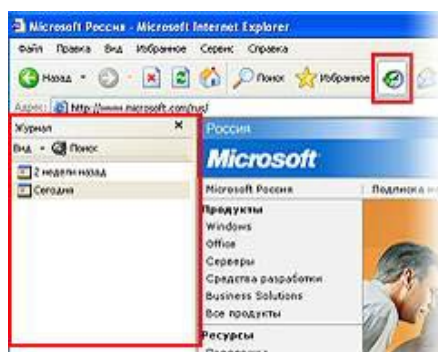
2. *Настройте параметры безопасности Интернет-обозревателя.*

Увеличить степень защиты можно также с помощью Интернет-обозревателя (браузера). Internet Explorer 6 дает возможность управлять системой защиты и степенью конфиденциальности данных при помощи присвоения сайтам уровней безопасности. Internet Explorer 6 помогает также соблюдать конфиденциальность данных во время посещения сайта, поскольку браузер будет отслеживать все действия сервера.

Отбор сайтов для посещения детьми

Невозможно всегда находиться рядом с детьми, когда они путешествуют по Интернету. Однако есть возможность проверить, на каких сайтах они проводят время. Для этого нужно:

- щелкнуть на кнопку «Журнал» на панели инструментов Internet Explorer. 
- затем выбрать папку, чтобы раскрыть ее, и просмотреть те сайты, которые посетил ребенок.



– просмотреть страницы, которые посетил ваш ребенок на конкретном веб-узле.

С помощью средств родительского контроля в MSN 9 можно получать по электронной почте еженедельный отчет о действиях вашего ребенка в Интернете. Вы узнаете общее время, проведенное в Сети; сайты, которые он посетил или пытался посетить; адреса электронной почты; имена людей, с которыми он обменивался сообщениями в MSN Messenger и файлы, которые он скачивал.

Меры предосторожности для общения в Интернете с незнакомцами

Чаты и система обмена мгновенными сообщениями предоставляют детям замечательные возможности для обсуждения интересующих их тем и установления дружеских контактов. Однако анонимность Интернета может представлять серьезную опасность; ваш ребенок рискует стать жертвой обманщиков и преступников. Научите детей предпринимать следующие меры предосторожности:

- представляясь, следует использовать только имя или псевдоним;
- никогда нельзя сообщать свой номер телефона или адрес;
- никогда не посылайте свои фотографии;
- никогда не разрешайте детям встречаться со знакомыми по Интернету без контроля со стороны взрослых.

Для предотвращения попыток контакта с вашими детьми со стороны незнакомых людей во время обмена мгновенными сообщениями настройте программу так, чтобы были доступны только проверенные контакты.

Для блокирования неизвестных контактов в Windows Messenger необходимо:

1. щелкнуть по кнопке *Сервис*.
2. далее выбрать *Свойства обозревателя*.
3. перейти на вкладку *Конфиденциальность*.
4. добавить тех, чьи адреса известны, в список *Разрешить* и *заблокировать всех других пользователей*.

Среди функций MSN 9 есть возможность ограничить переписку по электронной почте.

Практическое занятие 1. Повышение уровня безопасности детей в Интернете при помощи программных средств

В данном разделе речь идет о повышении безопасности для операционной системы Microsoft®Windows® XP Service Pack 2.

1. Центр обеспечения безопасности

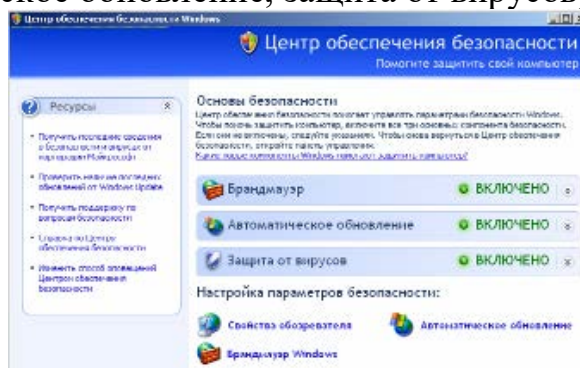
Если на компьютере установлена операционная **система Microsoft®Windows® XP Service Pack 2**, то можно использовать Windows Security Center (Центр обеспечения безопасности). Эта программа позволяет просматривать информацию о состоянии защиты компьютера и изменять настройки, а также получать дополнительные сведения по вопросам безопасности. Security Center показывает состояние трех важных компонентов безопасности:

- брандмауэра Интернета,
- антивирусных программ
- и службы автоматического обновления.

Кроме того, он служит для перехода к другим разделам безопасности, а также поиска технической поддержки и ресурсов, имеющих отношение к защите компьютера. Security Center работает в фоновом режиме, постоянно проверяя состояние трех наиболее важных компонентов.

Для того чтобы повысить уровень общей безопасности в Windows XP, нужно проделать следующие действия:

- нажмите кнопку Пуск/Start;
- в открывшемся меню выберите Панель управления/Control Panel;
- в панели управления откройте Центр обеспечения безопасности/Security Center;
- убедитесь, что включены основные компоненты безопасности (брандмауэр, автоматическое обновление, защита от вирусов).



Включить или отключить брандмауэр и автоматическое обновление вы можете непосредственно в **Центре обеспечения безопасности**. Для управления защитой от вирусов обратитесь к настройкам установленного антивирусного программного обеспечения.

Установите на вашем компьютере антишпионские настройки или дополнительное антишпионское программное обеспечение. Шпионскими программы могут существенно замедлить работу системы и привести к нежелательным изменениям в важных настройках. Такие программы трудно удалить. **Антишпионское программное обеспечение** поможет избавиться от шпионских и других нежелательных программ. Проверка компьютера может выполняться по расписанию в удобное время.

Для предотвращения появления шпионского программного обеспечения на компьютере, необходимо включить основные средства Центра обеспечения безопасности вашей операционной системы.

Для удаления шпионского программного обеспечения, попавшего на ваш компьютер, следует воспользоваться специальным антишпионским программным обеспечением, например, следующими программами: Windows Defender; Malicious Software Removal Tool. Эти бесплатные программы вы можете загрузить с сайта <http://www.microsoft.com/downloads> . Для этого в строке Search, в выпадающем списке необходимо выбрать All Downloads, в строке справа ввести название одного из указанных выше продуктов и нажать кнопку Go.

Задание 1. Скачайте одно из перечисленных ПО, установите и проверьте наличие шпионских программ на своем компьютере.

Рекомендуется: Для повседневной работы использовать учетную запись с ограниченными правами.

2. Блокирование доступа к нежелательной информации

Один из наилучших способов защиты от нежелательной информации - это блокирование доступа еще до того, как она может быть получена. Microsoft предлагает несколько таких способов.

2.1. Для того чтобы блокировать доступ к нежелательной информации в Internet Explorer® и MSN Explorer, нужно выполнить следующее:

- нажать кнопку Пуск/Start;
- в открывшемся меню выбрать Панель управления/ Control Panel;
- в панели управления открыть Свойства обозревателя/Internet Options;
- в появившемся окне перейти на вкладку Содержание/Content;
- в разделе Ограничение доступа/Content Advisor нажать кнопку Включить/Enable;
- в появившемся окне ввести пароль, который будет защищать вводимые ограничения;
- в окне Ограничение доступа/Content Advisor указать блокировку уровня доступа к нежелательной информации.

2.2. Для повышения уровня безопасности при работе ребенка с электронной почтой Outlook®Express.

- в меню программы Outlook® Express в разделе Сервис/Tools выбрать команду Параметры/Options;
- перейти на вкладку Безопасность/Security;
- при помощи переключателя выбрать зону безопасности для Internet Explorer/Select the Internet Explorer security zone to use , для того чтобы уменьшить вероятность появления вирусов на компьютере;

– также можно запретить сохранение или открытие вложений которые могут содержать вирусы: переключатели Не разрешать сохранение или открытие вложений, которые могут содержать вирусы/Do not allow attachments to be saved or opened that could potentially be a virus.

Если же вирус все же попал на ваш компьютер, то ограничить его дальнейшее распространение можно установив галочку Предупреждать, если приложения пытаются отправить почту от моего имени/Warn me when other applications try to send mail as me.

Для защиты пересылаемых писем от подделки и от возможности перехвата и прочтения кем-либо кроме указанного получателя, есть возможность выбрать команды Шифровать содержимое и вложения всех исходящих сообщений/Encrypt content and attachments for all outgoing messages и Подписывать все отправляемые сообщения/Digitally sign all outgoing messages.

Задание 2. Установите защиту Outlook® Express на своем компьютере, согласно перечисленным пунктам.

2.3. Заблокируйте поступление спама.

Чтобы блокировать поступление спама, необходимо воспользоваться почтовым сервером, имеющим защиту от спама или почтовым клиентом, имеющим спам-фильтр. Чтобы настроить спам-фильтр для почтового ящика, размещенного на сервере, необходимо зайти в этот почтовый ящик, и изменить настройки фильтра: добавить любого отправителя в список заблокированных (нежелательных), при этом почта от этого отправителя не будет поступать в ваш почтовый ящик. Если ваш почтовый сервер не имеет фильтра нежелательной почты, можно воспользоваться фильтром, встроенным в Microsoft Outlook.

Для настройки фильтра нежелательной почты в меню Microsoft Outlook необходимо:

- в меню выбрать Сервис / Tools;
- далее в открывшемся меню выбрать команду Параметры / Options;
- в открывшемся диалоговом окне перейти на вкладку Настройки / Preferences и нажать кнопку Нежелательная почта / Junk E-mail;
- в появившемся диалоговом окне внести изменения в настройки фильтра нежелательной почты.

Кроме того, вы можете воспользоваться спам-фильтрами других разработчиков.

Задание 3. Настройте фильтр нежелательной почты почтовой программы на своем компьютере.

2.4 Создание отдельных учетных записей.

Windows XP позволяет создать несколько учетных записей. Каждый пользователь сможет входить в систему независимо и иметь уникальный профиль с собственным рабочим столом и папкой Мои документы. Родитель может создать себе учетную запись администратора, дающую полный контроль над компьютером, а детям — ограниченные учетные записи. Пользователи с ограниченными учетными записями не смогут изменить системные настройки или установить новое аппаратное или программное обеспечение включая большинство игр, медиаплееров и программ поддержки чатов.

Для того чтобы создать отдельную учетную запись для ребенка с ограниченными правами доступа для работы в Интернете, необходимо выполнить следующие действия:

- нажать кнопку Пуск / Start, в открывшемся меню выбрать Панель управления / Control Panel;
- в панели управления открыть Учетные записи пользователей / User Accounts;
- в открывшемся окне выбрать Создание учетной записи / Create a new account, ввести ее имя;
- на этапе выбора типа учетной записи установить переключатель в положение Ограниченная запись / Limited;
- после нажатия кнопки Создать учетную запись / Create Account процесс создания учетной записи с ограниченными правами будет завершен.

Задание 4. Создайте на своем компьютере 3 учетные записи с разными ограничениями.

И в заключении, пароли — это ключи, которыми можно разблокировать компьютер и учетные записи в Интернете. Чем надежнее пароль, тем лучше защита от вторжения хакеров и мошенников, которые могут воспользоваться вашими личными данными в корыстных целях, например, открыть новые счета кредитных карт, обратиться за ипотекой или даже общаться через Интернет от вашего имени.

Путешествие по Сети может быть и развлечением, и полезным занятием, и способом общения как для взрослых, так и для детей. Однако важно, чтобы все новые пользователи Интернета, которых также называют Netizens, помнили о том, что они в Интернете не одни и, как и в реальной жизни, в Сети существуют правила поведения, или этикет, который необходимо соблюдать.

Вопросы:

1. Какие способы, помогающие защитить компьютер от опасностей в Интернете, Вам известны?
2. Какими должны быть «внутренние правила» использования Интернета?
3. Для чего предназначено антишпионское программное обеспечение?

4. Как можно следить за тем, какие веб-узлы посещают дети?
5. Следует ли детям разрешать иметь свои учетные записи электронной почты?
6. Какими способами можно заблокировать поступление спама?
7. Какую учетную запись рекомендуется использовать для повседневной работы?

Глоссарий

Спам – это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный Интернет-трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений, вредоносные программы

Кибермошенничество – это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя, с целью получить материальную прибыль. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг.

Коммуникационные риски – риски связаны с межличностными отношениями Интернет-пользователей и включают в себя контакты педофилов с детьми и киберпреследования.

Незаконный контакт – это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.

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

Блокирование доступа к неподходящим материалам – это один из способов защиты от нежелательной информации еще до того, как она может быть получена.

Фишинг – это один из видов мошенничества, направленный на хищение ценных личных данных пользователя, таких как номера кредитных карт, пароли, сведения о банковских счетах и др. Мошенники могут рассылать огромное количество сообщений, которые отправлены якобы надежными веб-узлами (например банка или компании-эмитента кредитных карт) и содержат запрос личных сведений.

Интернет-этикет, или «нетикет» – правила надлежащего поведения в киберпространстве.

Чат – открытая дискуссионная группа в Интернете, в которой можно общаться с другими людьми в режиме реального времени, используя псевдоним. Чатам и группам чатов часто присваиваются названия на основе темы или возрастной группы. В обсуждении может участвовать множество пользователей, но часто также возможно личное общение между двумя пользователями.

Гриферы – Интернет-хулиганы, получающие удовольствие от хамства и грубости, проявляющихся по отношению к окружающим.

Интернёт-зависимость (пишется с маленькой буквы через дефис; англ. Internet addiction, IA или англ. Internet addiction disorder, IAD) – психическое расстройство, навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета.

Веб-серфинг – бесконечные путешествия по Всемирной паутине, поиск информации.

Игровая зависимость - навязчивое увлечение компьютерными играми по сети.

Киберсексуальная зависимость – навязчивое влечение к посещению порносайтов и занятию киберсексом.

Шпионскими называются программы, выполняющие определенные действия (например, сбор личной информации или изменение настроек) без согласия и контроля пользователя. Они могут существенно замедлить работу системы и привести к нежелательным изменениям в важных настройках.

Антишпионское программное обеспечение – специальные программы, которые помогают избавиться от шпионских и других нежелательных программ. Проверка компьютера может выполняться по расписанию в удобное время.

Спам (нежелательная почта) – почтовое сообщение не имеющее информационной ценности для получателя, содержащие рекламную информацию, вирусы т.п.

Флейм – затяжной, эмоциональный спор в виртуальном общении.

Netizens – так называют всех новые пользователи Интернета.

Договор о правилах поведения при работе в Интернете

Я обязуюсь:

– Разговаривать со своими родителями, чтобы изучить правила пользования Интернетом, включая веб-узлы, которые я могу посещать, что мне можно делать, когда я могу выходить в Интернет, и сколько времени я могу работать в Интернете (___ мин. или ___ ч.).

– Никогда не сообщать свои личные данные, такие как домашний адрес, номер телефона, место работы или рабочий номер телефона моих родителей, номера кредитных карт, название или местоположение моей школы без разрешения родителей.

– Всегда немедленно сообщать родителям, если я увижу или получу в Интернете что-либо, что меня смутит или напугает, включая сообщения электронной почты, веб-узлы или даже обычную почту от моих Интернет-друзей.

– Никогда не соглашаться на личную встречу ни с кем из людей, с которыми я познакомился в Интернете, без разрешения родителей.

– Никогда не отправлять свои фотографии или фотографии членов моей семьи другим людям по Интернету или по обычной почте без согласия родителей.

– Никогда не сообщать мои Интернет-пароли никому, кроме родителей (даже лучшим друзьям).

– Не совершать в Интернете действий, которые могут нанести вред или раздражать других людей либо противоречат закону.

– Никогда не загружать, не устанавливать и не копировать ничего с дисков или из Интернета без соответствующего разрешения.

– Никогда не совершать в Интернете действий, которые требуют оплаты, не получив сначала разрешение от родителей.

– Разрешить родителям знать мои имена для входа на веб-узлы и псевдонимы для общения в Интернете, приведенные ниже:

Имя (ребенок) _____ Дата _____

Родитель или опекун _____ Дата _____

ПАМЯТКА безопасности для пользователя домашнего компьютера

- ограничить физический доступ к компьютеру, установить пароль на вход в систему и отключать доступ в Интернет, когда он не нужен;
- подписаться на информационные бюллетени Microsoft и регулярно обновлять операционную систему;
- отключить все неиспользуемые службы и закрыть порты, через которые могут осуществляться атаки;
- тщательно настроить все программы, работающие с Интернет, начиная с браузера — например, запретить использование Java и ActiveX;
- установить и обновлять антивирусную программу;
- использовать брандмауэр, хотя бы встроенный в систему, и внимательно анализировать его сообщения и логи;
- крайне аккуратно работать с почтой, а также программами для обмена сообщениями и работы с файлообменными сетями, например, следует отключить использование HTML в принимаемых письмах;
- никогда не запускать программы сомнительного происхождения, даже полученные из заслуживающих доверия источников, например, из присланного другом письма;
- ни при каких условиях не передавать по телефону или по почте свои персональные данные, особенно пароли;
- регулярно создавать резервные копии критических данных.

Если вы заметили, что ваш компьютер ведет себя «подозрительно»:

- Не паникуйте! Не поддаваться панике — золотое правило, которое может избавить вас от потери важных данных и лишних переживаний.
- Отключите компьютер от интернета.
- Отключите компьютер от локальной сети, если он к ней был подключен.
- Если симптом заражения состоит в том, что вы не можете загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows, который вы создавали при установке операционной системы на компьютер.
- Прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы на внешний носитель (дискету, CD-диск, флэш-карту и пр.).
- Скачайте и установите пробную или же купите полную версию Антивируса Касперского Personal, если вы этого еще не сделали и на вашем компьютере не установлено других антивирусных программ.
- Получите последние обновления антивирусных баз. Если это возможно, для их получения выходите в интернет не со своего компьютера, а с незараженного компьютера друзей, из интернет-кафе, с работы.
- Лучше воспользоваться другим компьютером, поскольку при подключении к интернету с зараженного компьютера есть вероятность отправки вирусом важной информации злоумышленникам или распространения вируса по адресам вашей адресной книги.
- Установите рекомендуемый уровень настроек антивирусной программы.
- Запустите полную проверку компьютера.