О ДЕТЯХ В ИНТЕРНЕТЕ

Основы детской безопасности
в «цифровом мире»

Пособие для родителей и учителей

16+

ЦЕНТР БЕЗОПАСНОГО ИНТЕРНЕТА

НЕ ДОПУСТИ!

РОЦИТ

ОБЩЕСТВЕННАЯ ПАЛАТА РОССИЙСКОЙ ФЕДЕРАЦИИ
CIVIC CHAMBER OF THE RUSSIAN FEDERATION

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES
INHOPE
ins@fe

ОГЛАВЛЕНИЕ

УВАЖАЕМЫЕ РОДИТЕЛИ И УЧИТЕЛЯ!

Наш нынешний век давно стал «цифровым» - электронные технологии давно и уверенно заняли привычное место в нашей жизни, наравне с обычным телефоном, газетами, автобусом и кухонной плитой. Эти «электронные технологии» стали подчас незаменимыми во многих аспектах повседневной деятельности – в коммуникации, получении информации, при совершении покупок, в развлечениях, и так далее до бесконечности. Логично, что новые технологии не могли не привлечь внимание преступников всех мастей, породив необходимость повседневных мер предосторожности – таких же, какие мы предпринимаем в оффлайне.

Одни из самых активных пользователей цифровых технологий – дети и подростки. При этом цифровые сервисы для них настолько привычны, что они зачастую не представляют себе, что когда-то можно было обходиться без них. Проникновение компьютерных и мобильных сервисов в подростковую среду сейчас приблизилось к ста процентам. Однако недостаток жизненного опыта и повышенная доверчивость делают несовершеннолетнюю аудиторию одной из самых уязвимых для различных «цифровых опасностей». В результате в обществе возникла новая цель – повысить уровень защищенности детей от многочисленных вредоносных явлений в Интернете, обучить детей азам «цифровой безопасности», помочь родителям и детям создать совместное безопасное «цифровое пространство» в семье. Именно на это направлена наша брошюра – более того, мы надеемся, что она может быть полезна Вам не только как родителям, заботящимся от защите своих детей, или учителям и воспитателям, но и просто как пользователям Интернета.

Эта брошюра не только поможет Вам организовать процесс обучения Ваших детей безопасной работе в Интернете, но и снабдит Вас дополнительными знаниями в области интернет-безопасности, которые пригодятся Вам как в беседах с Вашими детьми, так и в Вашей повседневной работе в Интернете.

Искренне надеемся, что наше краткое повествование сможет ответить на Ваши вопросы насчет работы детей в Интернете, поможет Вам и Вашим детям представить Всемирную Сеть лучше и сделает пребывание в Интернете более безопасным.

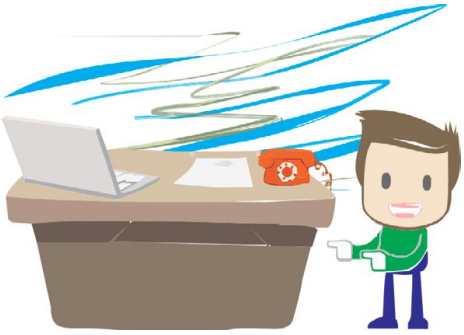
Центр Безопасного Интернета в России
Центр детской безопасности
в информационном обществе «НеДопусти!»

ЗНАКОМСТВО С ВИРТУАЛЬНЫМ МИРОМ

ЧТО ТАКОЕ КОМПЬЮТЕР И ИНТЕРНЕТ

Современный компьютер представляет собой мощный многофункциональный технический и информационный центр, способный решать задачи обучения, развлечения, поиска и обработки информации, помощи в производственных и вычислительных процессах. Все это, как бы парадоксально это ни звучало еще двадцать лет назад, с полным правом относится к обычному домашнему компьютеру. Подключение домашнего компьютера к сети Интернет увеличивает его возможности в десятки раз. Даже в базовой конфигурации современный компьютер может одновременно заменить телевизор, музыкальный центр, газеты, библиотеку, музей, справочную службу, игровую площадку, казино, клуб, телефонную компанию, почтовую службу и многое другое.

Для большинства российских детей дом по-прежнему является основным местом выхода в Интернет. Другими местами доступа во Всемирную сеть, более характерными для небольших городов и регионов со слаборазвитой инфраструктурой, являются кол-



лективные пункты доступа в Интернет (Интернет-кафе), компьютеры друзей, в ряде случаев – школьные компьютеры. Весьма популярным стал выход в Интернет посредством мобильной связи, которая есть практически в каждом регионе. В связи с этим предлагаемые советы по безопасности относятся не только к работе на домашнем компьютере – крайне желательно, чтобы ребенок осознавал, что правила безопасной работы в Сети обязательны в любом месте и при любом способе выхода в Сеть, в том числе (и в первую очередь) при выходе со смартфона или планшета.

Следует учесть, что в разговоре понятие «компьютер» часто оказывается очень расширительным. Обычно под собственно компьютером понимают **системный блок**, содержащий в себе все основные элементы, обеспечивающие работу компьютера. К их числу относятся процессор (устройство, обрабатывающее основные процессы в компьютере), оперативная память (ее величина нередко определяет быстродействие некоторых программ на конкретном компьютере), так называемый «жесткий диск» или «винчестер» - стационарное хранилище информации на компьютере, видеокарта и звуковая карта – специальные платы, отвечающие за отображение видео или звука соответственно. Внешними хранилищами информации могут быть компакт-диски (CD или DVD), читаемые компьютером через CD- или DVD-дисковод, а также так называемые «флэшки» - миниатюрные устройства для хранения информации (файлов), вставляемые в специальные гнезда (слоты). На совсем старых моделях компьютеров могут также присутствовать дисководы для 3-дюймовых дискет, служивших для переноса небольших объемов информации. Доступ в Интернет осуществляется с помощью сетевой карты (специальной платы для высокоскоростных или локальных соединений). К внешним устройствам относятся монитор, звуковые колонки (если имеются), клавиату-

ра и кнопочный манипулятор «мышь», а также «веб-камера» - компьютерная видеокамера (если есть).

Так «выглядит» стационарный персональный компьютер. **Моноблок** – не менее популярная форма стационарного компьютера – отличается от последнего только тем, что у него системный блок и монитор находятся в одном корпусе. В **ноутбуках** – переносных компьютерах, которые в последние годы серьезно потеснили «классические» компьютеры - все, кроме мыши, объединено в одном корпусе. Старые ноутбуки предназначались для путешествий деловых людей и потому большой мощностью не отличались – она была им просто не нужна. Однако в последние годы ноутбуки резко «прибавили» в мощности и не очень отличаются от стационарных машин, став пригодными даже для компьютерных игр, поэтому их все чаще используют в качестве основного домашнего компьютера – вместо «классических» ПК. Впрочем, есть и небольшие ноутбуки, ориентированные по-прежнему на бизнесменов-путешественников и минимум деловых программ, а потому обычно маломощные – нетбуки.

Практически сразу практика развития компьютерных и Интернет-технологий показала, что эти технологии используются отдельными людьми и сообществами также во вредоносных целях. Такие явления сейчас принято называть «цифровые угрозы» или «Интернет-угрозы», т.е. опасности, угрожающие посредством компьютерных и Интернет-технологий. Классификаций Интернет-угроз в настоящее время существует много – в зависимости от критерия, однако одной из старейших является классификация в зависимости от типа угрозы:

- ПРОГРАММНО-ТЕХНИЧЕСКИЕ УГРОЗЫ – опасности, в основе которых лежит вредоносный программный код, то есть некая программа, написанная для того, чтобы заставить компьютер совершать некие причиняющие вред действия.

- КОНТЕНТНЫЕ УГРОЗЫ – опасности, которые несет распространяемая в Интернете информация (по-английски «контент»). В

отличие от программно-технических, эти угрозы опасны непосредственно для человека – его повседневной жизни и мировосприятия. Один блок контентных угроз составляют порочащие человека тексты и изображения или такой контент, который может в будущем негативно повлиять на репутацию человека (например, порнографическая съемка). Другой блок воздействует на мировоззрение личности, изменяя его в деструктивную сторону – от экстремистской и сектантской пропаганды до «виртуальных клубов самоубийц». Особенно опасна такая информация для детей, потому что у них мировоззрение еще только формируется и они более восприимчивы к подобному контенту по сравнению со взрослым. Отдельно стоят оскорбления в Интернете и кибертравля, нередко приводящая к фатальным последствиям.

- ЭКОНОМИЧЕСКИЕ УГРОЗЫ – традиционно выделяются в отдельный вид угроз, так как включают в себя и программно-технические, и контентные элементы. Объединяет их объект атаки – виртуальный или реальный кошелек. Сюда включаются комбинации по краже денег в Интернете, в том числе с кредитных карт при покупках (виртуальный кардинг), кражи «виртуальных денег», мошеннические сайты, в том числе мошенничество под видом Интернет-магазинов.

Несколько особняком стоит **спам** – незапрошенная рассылка по электронной почте, способная содержать в себе Интернет-угрозы либо просто «растворять» среди кучи подобных сообщений полезную переписку.

ВРЕДНЫЕ ПРОГРАММЫ

Вредные программы как раз и представляют собой программно-технический блок Интернет-угроз. Как уже говорилось, программно-технические угрозы характеризуются нанесением вреда пре-

имущественно через программную и техническую инфраструктуру компьютера, вызывая те или иные вредные последствия. К их числу, например, относится искусственное замедление или затруднение работы компьютера, самопроизвольное выключение компьютера или создание технической невозможности его работы, а также удаление или искажение файлов. Из числа других вредных последствий можно отметить включение компьютера в сеть, рассылающую спам или вредоносные программы, без ведома хозяина, кражу сохраненных на компьютере файлов (тайную пересылку их на чужой компьютер) – сюда же входит кража сохраненных паролей, и «удаленное управление» веб-камерой с целью тайной съемки всего, что находится в поле «зрения» ее объектива. В большинстве случаев такие программки называются «**вирусы**» (заражающие компьютер) или «**трояны**» (крадущие информацию), а также «**черви**» (сетевые вредоносные программы). Преимущественно вредоносные программы заносятся на компьютер через Интернет (включая электронную почту) или с других компьютеров через портативные средства передачи информации (дискеты, «флешки»). Отдельные вредоносные программы пишутся для мобильных устройств – ввиду того, что у них свои операционные системы.

Основным методом защиты от программно-технических угроз на домашнем компьютере является также программно-технический – использование соответствующего защитного программного обеспечения. В первую очередь речь идет о специальных антивирусных программах (антивирусах), которые, сканируя объект, способны распознать вредоносную программу и заблокировать ее доступ к компьютеру (поместить в «карантин» или удалить). Такую программу следует обязательно установить на компьютере или мобильном устройстве перед началом рабо-

ты в Интернете. Для смартфона или планшета потребуется особый тип антивируса - «мобильный антивирус». Следует учитывать, что, поскольку новые вредоносные программы возникают в Интернете ежедневно, Вашему антивирусу необходимо обновляться примерно с такой же частотой – он будет получать описания новых программных угроз. Для этого антивирус должен обязательно быть лицензионным (наличие в пиратской версии поддельного ключа доступа не гарантирует его работоспособности) и иметь связь с Интернетом. Сейчас, как правило, антивирусное программное обеспечение включает в себя комплексное решение по защите от программно-технических угроз, а также некоторых экономических (например, сайтов, использующих программно-технические методы для хищения денег) и даже контентных («черные» или «белые» списки сайтов, функция «родительского контроля» для детей).

При установке антивируса следует предусмотреть в его настройках опции, которые разрешают ему сканировать входящую и исходящую электронную почту, соединение с Интернетом, а также присоединяемые к компьютеру устройства (например, флешку или карту памяти). Это позволит обеспечить весьма эффективную программно-техническую защиту по всем «фронтам», по которым может прийти вредоносное ПО. При этом также целесообразно периодически проверять антивирусом жесткий диск компьютера или основную память мобильного устройства на предмет поиска ускользнувших от внешнего контроля вредных программ. Разумеется, что каждый файл, скачанный из Интернета или открываемый с «флешки», должен перед открытием также быть просканирован антивирусом. При подозрительной реакции антивируса такой файл открывать не следует – целесообразно попытаться его «вылечить» антивирусом, а при неудаче – поместить в «карантин» или удалить, т.к. ряд вредоносных программ начинают работать после их открытия пользователем.

Отслеживать Интернет-активность собственного компьютера или мобильного устройства, а также «давать добро» каждой кон-

кретной программе на соединение с Вашим компьютером (смартфоном, планшетом) или из него с Интернетом может программное решение, называемое **файрволл** (от англ. firewall – «огненная стена»). Его использование позволит запретить выход в Интернет незнакомым программам, среди которых могут оказаться «трояны» - файрволл при каждой попытке некоей программы соединиться с Вами или Интернетом запрашивает пользователя. Правда, грамотное использование файрволла – чтобы не запретить доступ полезной программе – требует определенного уровня знакомства с программами, установленными на Вашем компьютере. Особенно важна такая мера предосторожности при пользовании мобильным Интернетом, так как «безлимитные» тарифы на мобильный Интернет пока не столь распространены, и возникает реальный шанс опустошения Вашего мобильного счета.

Как уже говорилось, Интернет представляет собой самое круп-

ПОИСК В ИНТЕРНЕТЕ

ное пространство циркулирования и хранения информации в истории человечества. Информация в Сети (так сокращенно называют Интернет) располагается на сайтах – группах веб-страниц, на которых размещена некоторая доступная человеку информация текстового, звукового или визуального характера. По оценкам компании Netcraft, на 1 января 2014 года в Интернете содержалось свыше 861 млн. сайтов (!), каждый из которых может содержать в себе от одной до сотен веб-страниц. Прирост количества веб-сайтов, по оценкам этой же компании, за 2013 год составил 37%, а в 2012-м – все 50%. Для сравнения, в 2010 году сайтов в Сети было всего 170 миллионов.

Ориентироваться среди этого массива сайтов помогают так называемые поисковые сайты, или поисковики – анализирующие

тематический запрос пользователя и предлагающие возможные веб-страницы и сайты, потенциально содержащие нужную информацию. По исследовательским оценкам, свыше 80% посетителей сайтов приходят на них с поисковиков. Несмотря на то, что в последние годы, кроме поиска, эти порталы предлагают и другие услуги, в том числе электронную почту, прогноз погоды или спутниковые карты, наиболее важной их функцией по-прежнему остается поисковая.

Следует учитывать, что анализ (индексация) содержимого сайтов осуществляется поисковиками автоматически, без участия человека-оператора, и в соответствии с определенными программными алгоритмами. **Поэтому зачастую в результатах поиска присутствуют сайты по очень отдаленной или вообще не имеющей отношения к запросу тематике.** Это, как правило, вызвано как неизбежными огрехами в работе поисковых машин, так и намеренными действиями отдельных создателей сайтов с целью попадания в верхние позиции результатов поисковых запросов. Очень важно, чтобы ребенок при овладении навыками поиска был готов к подобному обороту событий. Для результативного поиска необходимо, чтобы ребенок умел грамотно формулировать поисковый запрос и при необходимости предлагал поисковику несколько вариантов запросов, что увеличивает шансы нахождения полезной информации.

С подобными «огрехами» поисковых запросов и машин нередко связано то, что ребенок при ответе на свой запрос получает ссылки на контент, ознакомление с которым в данном возрасте может нанести вред образованию и развитию ребенка. К примеру, при запросе «девочки» поисковик может предложить ему сайты с рекламой интим-услуг или порнографическим контентом, а запрос по истории Великой Отечественной войны приведет на сайт исламских экстремистов. Это касается как общей опции поиска по сайтам, так и поиска среди изображений или видео.

Частично эта проблема решается путем использования так называемых «**опций детского поиска**», предлагаемых рядом поис-

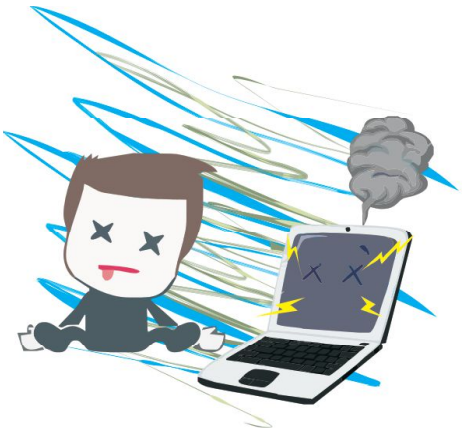
ковиков. В данном случае поисковый робот исключает из результатов поиска, предлагаемых пользователю, весь сомнительный с точки зрения допустимости контент. Однако следует четко осознавать, что любое автоматическое средство не дает стопроцентной гарантии исключения доступа ребенка к недопустимому контенту, а также то, что по некоторым вполне безобидным запросам поисковый робот может проявить «излишнюю бдительность» и отказать в удовлетворении запроса.

Ряд специализированных детских поисковиков предлагает поиск по определенным темам исключительно в пределах четко определенного круга допущенных сайтов. Как правило, таким образом исключается доступ к недопустимому контенту, но резко сужается пространство, из которого поисковик предлагает ребенку Интернет-информацию. Впрочем, на стадии обучения младших школьников работе в Интернете подобный поисковик дома является хорошим решением.

В случае, если ребенок пользуется обычным поисковиком, возможно использование **контентного фильтра** –программы, отфильтровывающей недопустимый контент по заранее заложенному списку или критериям. Фильтрационные опции могут также быть заложены в операционную систему или браузер (программу, которой пользуются для работы в Интернете и просмотра сайтов). Также при помощи этих программ возможно отследить, какие сайты были посещены ребенком. «Контентные фильтры» существуют и для мобильных устройств, в том числе в виде специальных «детских тарифов» - в которые изначально заложены ограничения на использование потенциально опасных сервисов. С учетом того, что мобильный телефон стал для детей главным способом обхода домашних ограничений на доступ к «нехорошему» контенту, необходимость соответствующей защиты для мобильных устройств становится очевидной.

Наиболее часто посещаемые или любимые страницы ребенок может сохранять в закладках браузера – специальной опции, предусматривающей сохранение адреса страницы (допустим,

www.site.ru) с целью быстрого перехода на эту страницу.



Если ребенок столкнулся с шокирующим его и противоправным контентом во время совместной с Вами работы в Интернете – необходимо как можно быстрее убрать с экрана шокирующее изображение или текст. Для того, чтобы убрать подобный сайт или страницу из Интернета удобным и анонимным способом, можно воспользоваться «**Горячей линией**» о противоправном контенте – в России такая линия была открыта в 2008 году Центром безопасного Интернета (проект под патронатом Общественной Палаты РФ) и доступна по адресу **www.nedopusti.ru.**

В веб-форме «Горячей линии» потребуется указать адрес страницы с противоправным контентом (Вы можете скопировать его из адресной строки Вашего браузера) и ту категорию противоправности, к которой, по Вашему мнению, она относится. Далее сообщение будет проверено аналитиками «Горячей линии» и, при наличии признаков противоправного контента, информация будет направлена к провайдеру с просьбой прекратить доступ пользователей к указанному контенту. При необходимости информация может быть передана в правоохранительные органы с целью совершения предусмотренных законом действий – например, выявления преступника. Информация о сайтах, размещенных за рубежом, передается российской «Горячей линией» в зарубежные «Горячие линии», входящие в сеть INHOPE (членом которой российская линия является с 2009 года).

Все сообщения принимаются анонимно. Своевременное сообщение о противоправном контенте в «Горячую линию» позволит уберечь других детей от столкновения с вредным для них контентом.

ОСНОВНЫЕ ПРАВИЛА:

- Следует обязательно пользоваться антивирусным программным обеспечением и файрволлом, обновляя их по их требованию;
- Все открываемые с внешних источников файлы должны проверяться антивирусом;
- Во избежание заражения следует проверять антивирусом жесткий диск (основную память) и внешние носители;
- Желательно предусмотреть опции специализированного детского поиска информации в Интернете и включать их во время работы ребенка в Сети;
- Очень желательно, особенно в младшем школьном возрасте ребенка, находиться рядом с ним во время работы ребенка в Интернете;
- При обнаружении неподходящего для ребенка контента – помочь убрать такой контент из Сети при помощи «Горячей линии».

ОБЩЕНИЕ В ИНТЕРНЕТЕ

ЭЛЕКТРОННАЯ ПОЧТА, СПАМ

Электронная почта (E-mail) является одним из наиболее ранних и быстрых средств коммуникации в Интернете. Почтовые сервисы позволяют практически мгновенно переслать текстовое сообщение, а также прикрепленные к нему текстовые, аудио-, видеофайлы или изображения адресату на другой конец земного шара. В настоящее время электронная почта активно применяется в личной переписке и деловой коммуникации. Практически все сервисы электронной почты, как правило, являются бесплатными.

Возможность пользования электронной почтой возникает с момента заведения собственного адреса электронной почты на одном из почтовых сервисов. Регистрация на таком сервисе, как правило, занимает 2-3 минуты. Разумеется, что электронное письмо можно отправить только тому, кто также имеет адрес электронной почты на любом из существующих почтовых сервисов. Типичный электронный адрес выглядит так: adres@servis.ru – значок @ является главным отличием адреса электронной по-

чты от адреса сайта.

Отправлять и принимать электронную почту можно как непосредственно в веб-формах почтовых сервисов в Интернете, так и при помощи специальных **почтовых клиентов** – программ, устанавливаемых на компьютерах и тем более на мобильных устройствах (например, для того, чтобы сводить в один центр письма с разных адресов электронной почты). Общаться по электронной почте сейчас возможно не только через стационарный компьютер или ноутбук, но также через смартфоны или планшеты, то есть по мобильной связи.

Как правило, при регистрации почтового ящика требуется указать некоторые персональные данные о себе. Настоятельно рекомендуется этого не делать и посоветовать ребенку обойтись псевдонимом; максимум реальных данных, которые могут быть указаны при регистрации – это имя, фамилия и возраст. Ребенок должен четко осознавать, что личная информация в Интернете является крайне уязвимой, и попадание таких данных к злоумышленникам (например, путем взлома серверов почтового сервиса) может негативно сказаться на Интернет-общении или реальной жизни ребенка (например, персональные данные могут стать отправной точкой для похищения ребенка).

Целесообразно посоветовать ребенку завести несколько почтовых ящиков на различных сервисах электронной почты и использовать каждый из них строго для определенных целей: например, один ящик – для общения с виртуальными друзьями, другой – для общения со знакомыми из реальной жизни. Во-первых, это поможет ему оставаться на связи в случае недоступности одного из почтовых сервисов; во-вторых, поможет легче избежать негативных последствий, если через один из ящиков ребенок станет объектом оскорблений, противоправных посягательств или прочих Интернет-угроз.

Базовым средством защиты электронной почты являются **логин** (электронный адрес) и **пароль** – только при их соответствии некто сможет попасть в почтовый ящик. Необходимо, чтобы ребенок четко осознавал, что **пароль от почтового ящика следует хранить в тайне – никому не говорить и не записывать**. Поскольку мошенники нередко обращаются с просьбами выслать пароль под видом администрации почтового сервиса, следует помнить, что в реальности ни одна почтовая служба ни под каким предлогом никогда не запрашивает пароли к ящикам пользователей. Забытый пароль можно восстановить при помощи соответствующих опций в почтовом сервисе.

Безопасный пароль должен быть достаточно длинным (не менее восьми символов) и включать в себя как минимум буквы и цифры. Это затрудняет подбор пароля наугад злоумышленниками. Именно поэтому нельзя делать пароли идентичными логинам, а также «лежащими на поверхности» и легко подбираемыми злоумышленником, имеющим минимальную информацию о ребенке – например, пароль из имени или фамилии ребенка. Специалисты советуют в любом случае периодически менять свой пароль, что повысит уровень защищенности почтового ящика Вашего ребенка.

Нужно ли, чтобы пароль от ящика ребенка знали Вы как родитель\опекун – решать Вам исходя из возраста ребенка, выбранной Вами модели воспитания и атмосферы, сложившейся в семье. Ряд специалистов рекомендует периодически проверять электронную почту ребенка, в том числе в его отсутствие, мотивируя это возможностью отследить негативное воздействие на ребенка (например, «завлечение» педофилом) на ранней стадии. Другие считают подобные действия нарушением права ребенка на личную неприкосновенность и стимулом к развитию у ребенка недоверия, скрытности, повышения нервозности.

Наиболее типичной Интернет-угрозой, связанной с электронной почтой, является **спам – незапрошенная пользователем рассылка электронных писем**. Спам составляет не менее 75% всех электронных писем, циркулирующих в Интернете, и в основ-

ном содержит рекламу неких товаров или услуг. Основных опасностей, связанных со спамом, две: посредством спамовых писем могут пересылаться вредоносные программы, опасные для Вашего компьютера (в связи с этим все письма следует проверять антивирусом), и заполненность почтового ящика ненужными письмами, среди которых становится очень сложно найти действительно нужную переписку. Спамовая атака, направленная на один конкретный адрес (например, злоумышленниками), способна вывести почтовый ящик из строя. Для ребенка опасность спама состоит еще и в том, что посредством него может распространяться недопустимый для ребенка в этом возрасте контент или его реклама, информация о его местонахождении (ссылка на сайт).

Простейшим способом защиты от спама является включение в настройках электронной почты **спам-фильтров** – фильтрационных решений, анализирующих письма и отсекающих явно похожие на спам. Как правило, спам-фильтр сортирует письма, помещая «полезные» в папку «Входящие», а те, которые он считает спамом, в папку «Спам» (иногда папки называются по-другому). В папке «Спам» письма по-прежнему доступны и могут быть перемещены из нее к «полезным» письмам непосредственно пользователем. Как и с контентными фильтрами, спам-фильтр не является стопроцентной панацеей и может пропустить спамовое письмо (особенно если оно замаскировано под личную переписку), либо, наоборот, отправить полезное письмо в спам. Совершенствование спам-фильтров минимизирует эту проблему с каждым годом, но она по-прежнему присутствует. Поэтому проверке пользователем подлежат все папки со входящими письмами – и нужно, чтобы об этом знал ребенок.

Можно также воспользоваться опцией сортировки Интернет-адресов – настроить спам-фильтр таким образом, чтобы он «пропускал» письма с определенных электронных адресов. Разумеется, такие настройки должны обновляться ребенком с изменением списка друзей у ребенка – и в случаях, если почтовый ящик друга используется кем-то для рассылки спама.

СРЕДСТВА ОБЩЕНИЯ В СЕТИ, ПЕРСОНАЛЬНАЯ ИНФОРМАЦИЯ

Развитие Интернет-технологий предоставило пользователям множество способов общения – причем вовсе не требующего программно-технических знаний. Среди наиболее типичных средств общения в Интернете, помимо электронной почты, можно отметить следующие:

- ЧАТ – возможность письменного общения в Интернете в режиме реального времени в рамках группы из нескольких человек;
- МГНОВЕННЫЙ МЕССЕНДЖЕР – возможность персонального письменного общения в режиме реального времени;
- ФОРУМ – возможность письменного общения (дискуссии) в рамках группы пользователей, допускаются большие по объему публикации-высказывания, общение может идти не в режиме реального времени;
- БЛОГ – возможность вести собственный открытый «интернет-дневник», который может читаться и комментироваться в режиме дискуссии различными группами читателей;
- МИКРОБЛОГ – рассчитан на быстрое размещение очень коротких сообщений, в режиме реплик или ссылок на другие онлайн-страницы. Другие пользователи, подписанные к микроблогу, немедленно получают опубликованную информацию и также могут в оперативном режиме ее комментировать;
- СОЦИАЛЬНАЯ СЕТЬ – возможность представлять в сети информацию о себе и путем просмотра аналогичных страниц находить друзей, устанавливать коммуникацию. Возможно выкладывание фотографий, аудио- и видеофайлов, ведение своего блога, игра в онлайн-игры.

Интернет-общение, в отличие от реального, имеет ряд специфических черт, о которых обязательно должен быть осведомлен ребенок. Большинство этих черт связаны с анонимностью персона-

жей, участвующих в дискуссии. К сожалению, никто не может гарантировать, что даже в социальной сети – где, казалось бы, анонимность минимальна из-за наличия фотографий и анкетных данных – мы видим данные и фото именно того человека, который в действительности ведет эту страничку. Этим нередко пользуются лица с преступными намерениями, в первую очередь мошенники – они добывают персональную информацию для краж или похищения ребенка – или педофилы, завязывающие знакомство с ребенком под видом его сверстника, втирающиеся в доверие и затем приглашающие ребенка на встречу, где и происходит посягательство на половую неприкосновенность.

Вопрос использования персональных данных, опубликованных в Интернете, во вред человеку, стоит исключительно остро. В связи с этим ребенок должен совершенно четко осознавать необходимость сохранения определенной анонимности в Сети.

Как правило, пользование любыми пользовательскими сервисами в Интернете, в том числе и средствами коммуникации, требует регистрации, подразумевающей возможность указания ряда персональных данных (фамилия, имя, отчество, возраст, домашний адрес, номер школы и класса, телефон). Ребенок должен четко осознавать, что в Интернет-средствах коммуникации указание реальных персональных данных не требуется. Максимум указываемых реальных персональных данных, допустимый для детских ресурсов – фамилия, имя и возраст.

При этом крайне желательно, чтобы ребенок в своем Интернет-общении пользовался псевдонимом. **Псевдоним** позволит защитить ребенка от нежелательной идентификации злоумышленниками и возможных последующих нежелательных действий, как-то: похищение несовершеннолетнего, ограбление родителей ребенка или вовлечение ребенка в сексуальную эксплуатацию. Однако важно, чтобы ребенок осознавал, что псевдоним в Интернете не является индульгенцией на недопустимые действия под прикрытием анонимности.

Несмотря на свободу выбора псевдонима, в этом деле у ребен-

ка должны присутствовать определенные этические ограничения. Как представляется, вряд ли следует ограничивать желание ребенка взять псевдоним по имени популярного киногероя. Однако к числу «недопустимых ходов» относятся попытки выдать себя в Интернете за лицо другого пола или возраста. Поэтому на попытки ребенка выдать себя, допустим, за взрослого в Интернете надо обращать соответствующее внимание и соответствующим образом их корректировать.

ДРУЖБА В ИНТЕРНЕТЕ: ОБЩЕНИЕ И ВСТРЕЧИ

Виртуальная дружба, завязываемая ребенком (равно как и взрослым) в Интернете, требует определенной осторожности, особенно на первых порах – во многом именно из-за того, что в Интернете собеседник легко может оказаться не тем, за кого себя выдает. Одно из главных правил безопасности, которое должен усвоить ребенок при работе в Интернете – что виртуальные друзья по возможности должны оставаться виртуальными. То есть это означает, что общение с друзьями, заведенными в Интернете, не должно выходить за пределы виртуального общения. Любая реальная встреча или более подробный обмен данными о себе у ребенка должен обязательно проходить под присмотром родителей, которые должны находиться как минимум поблизости и быть готовыми оказать физическую помощь при необходимости.

В связи с этим необходимо, чтобы ребенок четко осознавал возможную опасность виртуальных контактов. Для опытного педофи-

ла, к примеру, не составляет труда освоить детскую лексику, быть в курсе актуальных детских увлечений и с успехом выдавать себя на детском Интернет-ресурсе за ребенка. Поэтому крайне желательно, чтобы в семье возникло правило: обо всех приглашениях из виртуала ребенок должен рассказывать родителям и следовать их рекомендациям. Советы родителей или их плечо в нужный момент позволят ребенку избежать возможных крупных неприятностей, например не стать жертвой преступления.

Еще один важный момент, касающийся Интернет-общения, в том числе детского – поведение в Интернете. Удаленность от собеседника нередко провоцирует детей на нарушение установленных социальных норм поведения в связи с затрудненностью физических санкций. В результате дети нередко становятся жертвами кибероскорблений и кибертравли, зачастую не менее жестокой, чем в реальном мире, и не менее часто сами устраивают кибертравлю в отношении других пользователей.

В данном случае крайне важно, чтобы ребенок имел представление об институтах саморегулирования в Интернете и о степени их действенности. Закладывая в детскую культуру привычки решать вопросы культуры Интернет-общения через модераторов Интернет-ресурсов и иные институты саморегулирования, родители фактически закладывают основу для восприятия институтов гражданского саморегулирования в реальной взрослой жизни. Ребенок должен четко осознавать, что попытки восстановить справедливость по принципу «око за око» не только не являются продуктивными, но и не соответствуют званию культурного человека.

При этом на данный момент вряд ли стоит переоценивать действенность институтов саморегулирования на Интернет-ресурсах, так как они в данный момент находятся в стадии становления. Поэтому вполне адекватной является такая модель поведения, как уход с ресурса, где модераторы или администрация не принимают адекватных мер по защите пользователей. Ребенок должен ощущать, что «незаменимых сайтов нет», и в Интернете всегда можно найти удобное пространство с более дружелюбной и безопасной атмосферой.

ОБЩЕНИЕ В ИНТЕРНЕТЕ

В последнее время стали популярными (особенно среди молодежи) сервисы, в которых можно отмечать свое нахождение в некоторых местах («чекиниться», от английского «check in» - регистрироваться, «вписываться»). С одной стороны, чекины могут в определенной мере помогать родителям иметь представление о том, где находится ребенок – хотя это получится только при доброй воле ребенка, ведь чекин не происходит автоматически. С другой – информация о местонахождении человека может оказаться доступна и злоумышленнику. В результате, например, злоумышленники из сверстников смогут гораздо легче организовать некое опасное для ребенка или подростка действие, зная о том, где он находится в данный момент. Поэтому, как бы популярным ни было «чекиниться» в молодежной «тусовке», лучше порекомендовать ребенку воздержаться от этого увлечения. Тем более что самому ребенку это, как правило, «крутизны» не добавляет – а больше всего нужно администрации этих организаций, чтобы демонстрировать свою популярность по количеству и характеру чекинов.

ОСНОВНЫЕ ПРАВИЛА:

• При регистрации на сервисе электронной почты или любом пользовательском веб-сервисе следует оставлять о себе необходимый минимум персональной информации;

• Желательно пользоваться псевдонимом;

• Желательно иметь несколько адресов электронной почты для разных целей;

• Ящик электронной почты всегда должен быть защищен паролем;

• Пароль в Интернете должен быть в меру сложным и всегда храниться в тайне;

• Виртуальные друзья должны оставаться виртуальными;

• Реальные встречи с виртуальными друзьями должны проходить при участии родителей;

• Посторонним – то есть не членам семьи – совершенно незачем знать через Интернет, где ребенок находится в настоящий момент.

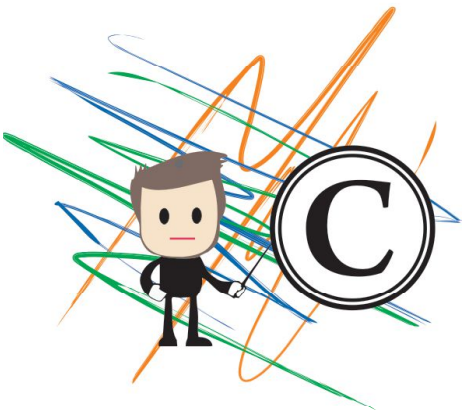
КАРТИНКИ И ВИДЕО В ИНТЕРНЕТЕ

КАРТИНКИ, МУЗЫКА И АВТОРСКИЕ ПРАВА

Одним из основных занятий детей в Интернете является поиск, публикация и скачивание из Интернета интересующих их картинок, видеоклипов, песен, фильмов. Поскольку развитие Интернет-технологий в настоящее время дошло до той степени, когда для совершения этих действий более не требуется специальных знаний в области программирования или обслуживания компьютеров, подобное увлечение стало массовым – в связи с чем в Сети возникло множество сервисов, помогающих публиковать и обмениваться аудио- и видеофайлами. Как правило, такие сервисы называют **аудио-** или **видеохостингами**.

Публикация контента на таких сервисах, как правило, относительно проста и требует в лучшем случае формальной регистрации. Не говоря уже о том, что наличие файловых хостингов избавляет многих пользователей от необходимости создавать собственный сайт для публикации некоего визуального или звуково-

го контента. Еще более простым является процесс потребления выложенного в Интернете (опубликованного) контента, включая его сохранение на компьютере или мобильном телефоне пользователя (скачивание).



Современная культура пользования информационными продуктами предусматривает **уважительное отношение к чужому интеллектуальному продукту**, что подразумевает возможность использования его только на определенных условиях. В современный период одним из таких условий нередко является определенная плата за пользование информационным продуктом.

Крайне желательно, чтобы ребенок осознавал, что плата за скачивание продукта является не прихотью правообладателя, а средством окупить свой труд и является аналогом зарплаты на производстве. В связи с этим плата за скачивание может являться также платой за удобство, так как поиск глубоко «спрятанных» в Интернете бесплатных ссылок может занять много времени и сил. Для того, чтобы ребенок мог пользоваться легальными сервисами скачивания контента, целесообразно завести специальный Интернет-кошелек с небольшой суммой, расходуя которую, ребенок сможет обучаться культурному и корректному потреблению Интернет-контента.

Другим исключительно важным моментом уважительного отношения к чужому интеллектуальному продукту является сохранение авторства продукта – то есть указание настоящего автора или источника при использовании того или иного текста, картинки, аудиовидеофайла. К сожалению, нередко, даже в учебном процессе, дети беззастенчиво заимствуют в Интернете чужие ранее написанные работы, меняя в них только имя и фамилию автора на свои. В других случаях за свои могут выдаваться якобы сделанные ребен-

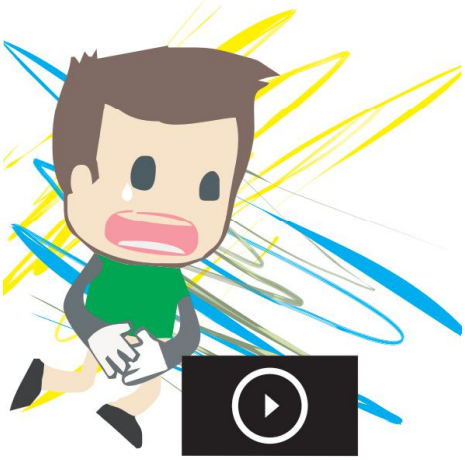
ком фотографии, поделки и прочее.

Наряду с привитием понимания недопустимости «кражи интеллектуального продукта», ребенку следует дать информацию о санкциях за подобные действия и, самое главное, об их реальности. Желательно, чтобы это иллюстрировалось понятными ребенку по его повседневной жизни примерами – как, например, возможный случай сдачи несколькими учениками одинаковых работ под своими именами и отрицательную реакцию учителя в форме неудовлетворительной оценки. Ребенок должен усвоить, что любые заимствования в учебной, научной и публицистической деятельности допускаются только с указанием автора и\или источника заимствования, в противном случае заимствование может считаться некорректным и даже противоправным – и в будущем повлиять на судьбу работы и самого «заимствователя».

КИБЕРУНИЖЕНИЕ И КАМЕРА

Явление киберунижения получило дополнительный толчок с развитием цифровых камер, дав, пожалуй, **самый опасный вид киберунижения – когда сцены унижения и насилия снимаются на камеру** (мобильного телефона, фотоаппарата, видеокамеры) **и затем публикуются в Интернете**. В настоящее время камера имеется у многих детей – как минимум в мобильном телефоне (ими обзавелись даже бюджетные версии мобильников). В результате сцены насилия приобретают особо унизительный, иногда сексуальный подтекст, процесс демонстрируется во всех подробностях. «Зонами риска», помимо улиц и задворков школ, являются также раздевалки школ и особенно спортзалов.

Подобные моменты киберунижения опасны тем, что со сценой унижения ребенка знакомится неограниченное число людей, и проблему психологических последствий для ребенка может не



решить даже переезд в другой город – ибо Интернет трансграничен, и никто не может дать гарантии, что раз опубликованная сцена насилия не «всплывет» в Сети через какое-то время. В связи с особой опасностью подобных форм киберунижения борьбе с ними должно быть уделено соответствующее внимание.

Как потенциальный обидчик, ребенок должен твердо усвоить недопустимость подобных действий, в том числе под угрозой санкций. Крайне желательно создать у ребенка ощущение **неотвратимости санкций** и их независимости от родителей, в том числе как приходящих по линии правоохранительных органов. Любой контент, обнаруженный на компьютере или мобильном телефоне ребенка и содержащий признаки киберунижения, должен становиться предметом тщательного изучения проблемы и – при необходимости – жестких санкций со стороны родителей.

С точки зрения жертвы ребенок должен иметь четкое представление о **возможных помощниках** в потенциальной кризисной ситуации. Во-первых, он должен быть уверен в помощи родителей и знать, что в кризисной ситуации к ним следует обращаться за помощью. Ни в коем случае не высмеивая ребенка, следует установить максимум подробностей и принять необходимые меры. Не следует стесняться требовать вмешательства со стороны школы, преподавательского сообщества, соответствующим образом привлекая учителей к решению проблемы личной безопасности детей в школе, а в конкретной ситуации – к наложению санкций на обидчиков. В критической ситуации к проблеме могут быть привлечены сотрудники правоохранительных органов, которые могут оказать необходимое воздействие на киберунизителей – более того, реагирование на подобные случаи со стороны правоохранителей входит в их должностные обязанно-

сти. Ребенку при необходимости может быть оказана психологическая помощь.

КАРТИНКИ, ФОТОГРАФИИ И БЕЗОПАСНОСТЬ

Потенциально противоправные способы использования веб-камер, цифровых фотоаппаратов и камер мобильных телефонов заставляют пользователей цифровых технологий и общество вообще предпринимать определенные шаги по защите от вредоносных действий с использованием цифровых камер. Помимо активной борьбы с киберунижением, на помощь пользователям приходит комбинация программно-технических защитных мер и поведенческих советов.

Ряд вредоносных программ в настоящее время обладает возможностью самостоятельно активировать веб-камеру, присоединенную к компьютеру или встроенную в компьютер, заставляя ее производить съемку без ведома хозяина и пересылать результаты съемки на компьютер злоумышленника. Наиболее надежным средством защиты от подобной напасти является обычное **антивирусное и «антишпионское» (anti-spyware) программное обеспечение**, то есть комбинация обычных антивируса и файрволла. Ряд пользователей по собственной инициативе принимают дополнительные меры предосторожности, например отсоединение веб-камеры от компьютера или закрытие ее объектива.

Впрочем, гораздо чаще злоумышленники – в данном случае педофилы – просят детей использовать веб-камеру сознательно, например для совершения перед камерой неких сексуальных действий. Как правило, подобные предложения поступают в видеочатах. Проблема показала себя достаточно массовой в Европе и США, где подобное предложение мог получить каждый шестой ре-

бенок. Разумеется, на такие «просьбы» следует соответствующим образом реагировать, в том числе с передачей информации об извращенце в правоохранительные органы. В большинстве случаев профилактика недопустимости подобных действий, которую можно провести с ребенком, не выходит за пределы общей пропаганды сексуальной этики и недопустимости развратных действий.

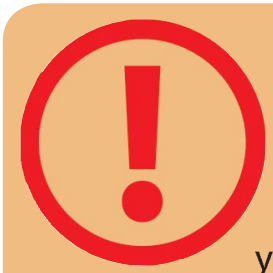
Несколько более широкий спектр проблем возникает в связи с фотографиями – ввиду большей легкости их изготовления, монтажа и пересылки. Дети достаточно активно обмениваются фотографиями и активно их публикуют на внешних ресурсах. С учетом того, что однажды опубликованное в Интернете крайне сложно удалить полностью, крайне важно, чтобы ребенок осознавал принцип «Что написано пером – не вырубишь топором» применительно к Интернету. А именно – очень важно научить ребенка корректной оценке изображения, которое он хочет выложить в Интернет. Ребенок должен осознавать, что опубликованные им фотографии, изображающие его с негативной стороны, однажды могут нанести ему вред, негативным образом сказаться на его жизни – причем это может случиться спустя годы.

В этой связи довольно крупную проблему стали составлять так называемые «**селфи**» - фотографии себя самого (самой), сделанные при помощи камеры собственного мобильного телефона. Причем не столько «селфи» как таковые, сколько их разновидность под названием «**секстинг**» - самостоятельная съемка эротических фото или видео на камеру собственного мобильника. Секстинг характерен не только для подростков (в основном девушек), но и для детей предподросткового возраста – убежденных, что такие изображения являются ключом к успешности в своем окружении и на публике вообще. Именно такие фотографии становятся основой для сексуальной эксплуатации и киберунижения несовершеннолетних, негативно влияя на их честь, достоинство и репутацию. Если с киберунижением все ясно – фото используется для оскорблений, массовой рассылки и служит причиной непристойных реплик и предложений – то с педофилами несколько сложнее: они могут

рассматривать такое фото как «приглашение» к грумингу (вовлечению в половые отношения), а также использовать его для шантажа с целью вовлечения ребенка в сексуальную эксплуатацию или получения более «откровенных» изображений. Главным способом профилактики таких инцидентов является укоренение у ребенка безусловного мнения о недопустимости и опасности поиска «популярности» подобными способами, с одновременным подсказыванием безопасных альтернатив обретения популярности.

Другая сторона тщательного подхода к публикации изображений – это ответ на вопрос «А что другие смогут узнать по моей фотографии?». Опытный аналитик, которых немало среди преступников, по изображенным предметам может довольно четко установить место проживания ребенка или его обучения, с целью выбора жертвы и совершения преступления. Причем преступление может быть направлено как против ребенка (похищение, сексуальная эксплуатация), так и против близких (например, ограбление). Великолепным «подарком» преступникам в таком случае может являться, например, крупный план школьной тетради с данными школы, или уличная табличка на доме с подписью к фото «Мой дом». Поэтому публикуемое фото должно быть максимально обезличено – во избежание возможного интереса преступников.

В последнее время весьма популярными, в том числе среди детей, являются Интернет-открытки – комбинация текстового поздравления, картинки и звукового файла. Современные Интернет-технологии и редакторы открыток позволяют ребенку скомпоновать поздравление своим друзьям и близким практически из любого изображения. Однако еще одно «не», которое ребенок должен знать при работе в Интернете – это недопустимость изменения изображений таким образом, чтобы они унижали достоинство изображенного. Даже дружеский шарж может унизить достоинство, если этот шарж не был согласован. **Поэтому на публикацию унижающих достоинство изображений ребенком однозначно должен быть наложен запрет.**



ОСНОВНЫЕ ПРАВИЛА:

• Уважение чужого авторства в Интернете – залог хорошей успеваемости в школе;

• Снимать и публиковать в Сети сцены насилия и унижения – недопустимо и наказуемо;

• Выкладывая фото или видео в Сеть, семь раз подумай, один раз публикуй;

• Лучше не публиковать то, что выставит человека в будущем в негативном свете;

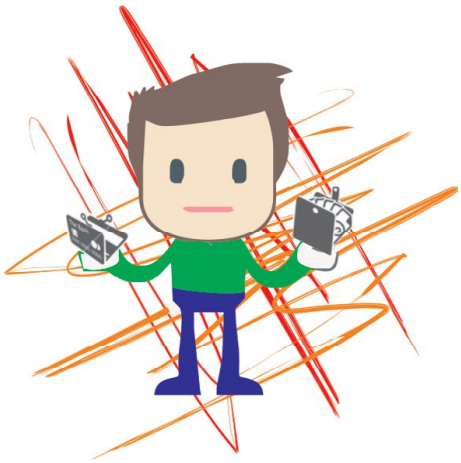
• «Непристойные предложения» с вебкамерами ребенок должен отклонять и рассказывать о них родителям, которые должны принимать меры вплоть до обращения к правоохранителям;

• Антивирус защитит от «скрытой съемки» без ведома хозяина камеры.

ПОВЕДЕНИЕ И ПОСТУПКИ В СЕТИ

ДЕНЬГИ В ИНТЕРНЕТЕ

Многие товарно-денежные сервисы достаточно прочно укоренились в Интернете, множество платных услуг оказывается через Сеть – начиная от «электронного банкинга» и кончая Интернет-магазинами, то есть возможностью удаленного приобретения товаров. Как правило, оплата услуг через Интернет осуществляется двумя способами. В первом случае платежным средством являются дебетовые и кредитные карты, указание данных которых позволяет осуществить списание с них денежных средств и, таким образом, приобретение товара или услуги. Во втором оплата осуществляется так называемыми «электронными деньгами» - платежными единицами электронных платежных систем, приобретаемыми заранее за наличные деньги либо по кредитным картам. Платеж в Интернете требует предварительной регистрации на сервисе, ввода логина и пин-кода (пароля), а также, возможно, иных подтверждающих действий.



В любом из этих случаев речь идет о реальных платежных средствах, требующих к себе такого же отношения, что и деньги в обычном кошельке. Именно поэтому политика доступности к «электронным деньгам» в семье должна как минимум соответствовать политике доступности к деньгам обычным. В первую очередь необходимо сформировать у ребенка четкое понимание того, что **в Интернете он имеет дело с реальными деньгами**, которые требуют к себе бережного отношения и произвольно тратить которые недопустимо. При этом необходимы определенные меры предосторожности во избежание самовольной траты ребенком электронных денег в качестве «игры». А именно: пароли от ящиков электронных денег должны сохраняться втайне от ребенка, любая платежная операция должна требовать ввода пароля, который не должен быть сохранен на сайте, и кредитные карты не должны попадать в руки ребенку.

Крайне желательно ограничить доступ ребенка к таким сервисам, как Интернет-аукционы, накладывающие на участника финансовые обязательства до фактического совершения платежа. Известны случаи, когда ребенок, уже понявший механизм аукциона, но еще не знающий ценности денег, совершал крайне неожиданные для родителей покупки.

Третьим аспектом, связанным с неправомерным использованием несовершеннолетними «электронных денег», является использование Интернета для приобретения вещей, которые несовершеннолетнему не продадут при личном визите в магазин. В первую очередь речь идет об алкоголе и, в меньшей степени, табачной продукции, а также платных порносайтах - и касается эта проблема обычно подростков, отдающих себе отчет в своих действиях. В России эта проблема пока развита слабо ввиду слабого развития продуктовых Интернет-магазинов, но, например, в США школьни-

ки неплохо освоили «путь обхода» через Интернет. Главным средством защиты является хранение данных кредитных карт в тайне.

При всем этом ребенок вполне может иметь собственный «кошелек» в электронной платежной системе, который создадут ему родители. Ограниченная «карманная» сумма должна использоваться ребенком на оплату объектов авторских прав (фильмов, музыки) и попутного обучения пользованию этими сервисами. Разумеется, контроль расходов должен осуществляться родителями, равно как родители должны контролировать и «финансовое поведение» ребенка в Сети – любые попытки ребенка каким-то образом «поднять деньги» должны пресекаться, так как они обычно способствуют развитию не предпринимательства, а мошенничества.

Вообще Интернет-мошенничество по-прежнему весьма распространено в Сети, причем есть группы мошенников, специализирующихся именно на детях. Понимая недоступность кредитных карт детям, мошенники предлагают отправить на некий «короткий номер» SMS-сообщение, в результате чего с мобильного счета списывается сумма, в десятки раз больше заявленной. Жертв заманивают якобы продажей картинок, музыки, видеороликов, предоставлением «премиум-доступа» или бонусов в онлайн-игре, более выгодным мобильным тарифом. Необходимо, чтобы ребенок знал о существовании в Интернете мошенников и относился к любым, даже самым выгодным предложениям отдать деньги в любой форме с недоверием. Лучше всего, чтобы заказ или покупка любых услуг через мобильную связь или Интернет осуществлялись совместно с родителями.

Впрочем, «денежные» опасности посредством мобильной связи этим не ограничиваются. Нередки случаи, когда мошенник, имитируя знакомого ребенку человека, срочно просит его о финансовой помощи под надуманным предлогом (вплоть до поиска средств на взятку якобы задержавшим его сотрудникам полиции). Как правило, имя «знакомого» подбирается наудачу, а рассылка (либо звонки) осуществляется массово – тоже «наудачу», в расчете на то, что среди знакомых получателя найдется хоть один человек с соот-

ветствующим именем. «Помощь» ожидается опять же через перевод денег с мобильного счета. Особо «продвинутые» мошенники могут подделать даже номер телефона – впрочем, обычно это делается ради крупных сумм и довольно редко грозит детям, такими суммами не располагающим. Также мошенник может прислать СМС или даже позвонить ребенку и представиться работником сотовой компании (мобильного оператора), предложив «новый мобильный тариф» или, наоборот, информируя о якобы имеющейся задолженности и требуя ее немедленно погасить.

Наилучшим способом профилактики такого мошенничества является контрольный звонок на номера тех знакомых, кто, по мнению ребенка, в данный момент обращается за помощью. При этом надо перезванивать на ранее известные номера, а не на номер, с которого позвонили или прислали СМС с просьбой о «помощи». В случае, если абонент по тем или иным причинам недоступен, ребенку лучше воздержаться от самостоятельного перевода денег. Компромиссом между «гражданской совестью» и боязнью быть обманутым может стать передача ребенком информации третьему хорошему знакомому из взрослых, который сможет гораздо лучше разобраться в ситуации. Если же мошенник звонит от имени мобильного оператора, следует позвонить в абонентскую службу мобильного оператора – их настоящие телефоны общедоступны – и поинтересоваться правдивостью информации применительно к мобильному счету ребенка. Поскольку мобильные номера зарегистрированы на взрослых, есть смысл, чтобы в абонентскую службу позвонили родители – что означает, что ребенок должен сообщить о неожиданном предложении отцу или матери.

ИНТЕРНЕТ-ЗАВИСИМОСТЬ

Интернет-зависимость на данный момент является, пожалуй, са-

мой известной Интернет-проблемой, не связанной с программно-техническими аспектами. Начинаясь с чрезмерного увлечения Интернетом, Интернет-зависимость может приобретать характер, схожий с наркотической зависимостью, а также длительное времяпровождение за компьютером может оказать негативное влияние на здоровье ребенка (нервная и мышечная системы, органы зрения и слуха, кровообращение). Разумеется, социализация ребенка в реальном мире приносится в жертву Интернет-увлечениям – исчезают друзья и увлечения в реальном мире, ребенок перестает уделять внимание школьным занятиям и выполнению домашних заданий. В итоге возникает риск формирования несоциализованной, то есть неадаптированной к окружающему миру, и физически больной личности, у которой могут также присутствовать проблемы со знаниями. Крайне тяжелая форма Интернет-зависимости – непрерывная работа за компьютером в течение длительного периода – может привести к летальному исходу. Множество описаний Интернет-зависимости, от просветительских до клинических, присутствуют в литературе и Интернете.

На первый взгляд Интернет-зависимость может показаться схожей с чрезмерным увлечением книгами или телевизором, что было свойственно предыдущим поколениям – однако это не так, ибо в этих случаях не возникало интерактива и глубокого «погружения в иную реальность». Предупреждение Интернет-зависимости в семье должно, по мнению специалистов, основываться на установлении четкого баланса между «виртуальным» и «реальным» «мирами», и одним из краеугольных камней здесь должен стать **график использования компьютера и Интернета.** Такой график может стать частью «семейного контракта», или семейных правил по пользованию Интернетом. Необходимо помочь создать условия, в

которых бы ребенок чередовал компьютерную работу с другими увлечениями – чтением, просмотром телепрограмм, слушанием музыки, спортивными состязаниями, времяпровождением с друзьями. Крайне желательно, чтобы чтение и просмотр фильмов осуществлялись в таком случае не за компьютером.

Если Вы замечаете у ребенка поведенческие изменения, связанные с чрезмерным времяпровождением в Интернете – целесообразно обратиться за помощью к психологу, который может назначить курс психологической реабилитации.

НЕТИКЕТ, ИЛИ ПРАВИЛА ХОРОШЕГО ТОНА В СЕТИ

В общем и целом работа и времяпровождение в Интернете предусматривают следование определенным нормам поведения. Часть из этих норм продиктована особенностями компьютерной коммуникации, большая же часть соответствует культурно-этическим нормам реального мира. Следование этическим нормам в Интернете обеспечивает успех в использовании Интернета и в социализации в Интернет-среде.

Процесс формирования этики поведения в «виртуальном мире» принципиально не отличается от формирования поведенческой модели ребенка в повседневной жизни и включает в себя тех же действующих лиц: главным образом семью и школу. Предполагается, что школьное участие, помимо общевоспитательной деятельности, будет также проявляться в ходе уроков компьютерной грамотности. Однако семейный вклад на данной стадии будет гораздо более основополагающим и будет носить как общевоспитательный характер, так и определенные действия, непосредственно связанные с компьютером и Интернетом. В принципе, это должны быть совместные с ребенком занятия за компьютером.

Ключевой постулат, от которого, на взгляд специалистов, должно отталкиваться формирование сетевого этикета ребенка («нетикета», от англ. net – Сеть и фр. etiquette – этикет) – «**Поступай так, как хочешь, чтобы поступали с тобой**». Эта упрощенная форма категорического императива немецкого философа И.Канта универсально позволяет соотносить совершаемые или планируемые действия с наиболее ценным для многих личностей мерилом – самим собой. При отсутствии правил, четко регламентирующих некий вопрос поведения в Сети, на наш взгляд, следует соотносить поступок с рекомендуемой общей нормой оффлайнового правильного поведения.

Остальные правила являются, как правило, специальными, то есть касаются конкретных сфер, ситуаций и поступков. К ним относятся соблюдение культуры и этики общения в Сети, следование правилам, установленным для пользования на конкретном Интернет-ресурсе, общие правила коммуникации (например, средства выражения эмоций при текстовой переписке). Здесь целесообразно обратить внимание на ложность тезиса о присутствии некоей «этики виртуального мира», отличной от этики поведения в повседневной жизни – дело в том, что **все действия, совершаемые в Интернете, человек совершает в реальной жизни**, ибо он физически не перемещается в некую иную реальность. В связи с этим важно, чтобы ребенок усвоил, что мораль и законы «реального мира» действуют – и обязательны! - и при работе в Интернете.

Необходимо, чтобы ребенок четко представлял себе, что и когда он имеет право делать за компьютером, а что и при каких обстоятельствах – нет. Для лучшей запоминаемости целесообразно порекомендовать способ, успешно зарекомендовавший себя в англосаксонских странах – занести правила использования ребенком Интернета на бумагу, в форме «**семейного контракта**» или «**семейных правил**» пользования компьютером. Такой документ следует составить вместе с ребенком как результат совместного обсуждения (односторонне навязанные правила ребенок, скорее всего, отторгнет) и включить в него график использования Ин-

тернета ребенком, основные условия, при которых можно продолжать работу в Сети (например, обязательное включение отдельных программ), а также правила, связанные с безопасностью. Документ не должен быть излишне конкретным – все-таки это не Уголовный кодекс, но при этом он должен охватывать все основные «проблемные точки» работы в Интернете. По сложным вопросам «Семейные правила» должны предусматривать обращение за помощью к родителям.

Следование подобным «Семейным правилам» вкупе с воспитательным процессом и защитными мерами помогут наиболее эффективно использовать Интернет для обучения и развития ребенка, создав базу для формирования ответственного и разумного пользователя Интернета. Само собой, что чем больше таких пользователей – тем, скорее всего, безопаснее будет в Интернете.

ОСНОВНЫЕ ПРАВИЛА:

• Следует обеспечивать тайну «электронных денег» от ребенка, а все личные аккаунты на подобных сервисах должны быть защищены паролем;

• Ребенок должен быть осведомлен о наличии Интернет-мошенников и знать, что ни при каких обстоятельствах нельзя никому отправлять никакие денежные переводы или платные SMS;

• Необходимо обращать внимание на длительность работы ребенка в Интернете и разницу его поведения за компьютером и в реальном мире. Если возникает Интернет-зависимость – необходимо связаться со специалистом;

• Формирование сетевого этикета ребенка – залог его безопасности в Интернете в настоящем и будущем;

• Желательно сформировать совместно «Семейные правила» использования компьютера и Интернета, которые будут понятны ребенку.

НЕ ДОПУСТИ!

РОЦИТ

СОПРОТИВЛЕНИЕ
правозащитное движение

ОБЩЕСТВЕННАЯ ПАЛАТА РОССИЙСКОЙ ФЕДЕРАЦИИ
CIVIC CHAMBER OF THE RUSSIAN FEDERATION

Уполномоченный при Президенте Российской Федерации по правам ребенка

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES
INHOPE
ins@fe

Co-funded by the EU under Safer Internet Programme

International Centre
FOR MISSING & EXPLOITED CHILDREN

KASPERSKY lab

При реализации проекта используются средства государственной поддержки, выделенные в качестве гранта в соответствии с распоряжением Президента РФ № 115-рп от 29.03.2013 г.

Safer Internet Centre is co-funded by the EU under Safer Internet Programme

По всем вопросам просьба обращаться на электронный адрес mail@nedopusti.ru.

©РОЦИТ, 2014. Тираж 3000 экз.

Распространяется бесплатно.

НЕ ДЛЯ ПРОДАЖИ