ОПАСНОСТИ И ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТЕ. ЧТО НУЖНО ЗНАТЬ ПЕДАГОГУ И РОДИТЕЛЯМ

Насколько готовы педагоги к новым формам обучения ивоспитания? Как они воспринимают возможности этих технологий?

Действительно, информационные и коммуникационныетехнологии открывают уникальные возможности для системыобразования, вместе с тем все большую актуальность приобретаетпроблема безопасности ребенка в информационном обществе,отличающемся информационной насыщенностью и интенсивностью,многоканальностью влияний, многообразием транслируемых ценностей. Е. С. Полат указывает на чрезвычайную опасность, которая кроется не столько в самом компьютере, сколько в доступной для всех желающих информации, размещенной в сетях.

Несмотря на то, что в школе безопасный доступ детей вИнтернет обеспечивается контентной фильтрацией нежелательной информации, созданием специальных образовательных сетей, содержание информации в которых контролируется системными администраторами, проблема обеспечения эффективного и безопасного использования Интернет требует дальнейшего серьезного осмысления в педагогической науке и конкретных действий в педагогической практике.

В России около 8 миллионов пользователей глобальной сети — дети. Они могут играть, знакомиться, познавать мир... Но в отличие от взрослых, в виртуальном мире они не чувствуют опасности. Наша обязанность — защитить их от негативного контента.

Перечислим основные опасности, которые связаны с использованием интернета. Их можно разделить на две группы,связанные: с техническим, программным оснащением компьютера и с личностными характеристиками ребенка.

Интернет-опасности, связанные с техническим оснащением компьютера

Контентные риски связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент.

Неподобающий контент. В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

Незаконный контент. В зависимости от законодательства страны разные материалы могут считаться нелегальными. В большинстве стран запрещены: материалы сексуального характера с участием детей и подростков, порнографический контент, описания насилия, в том числе сексуального, экстремизм и разжигание расовой ненависти.

Вредоносные программы. Вредоносные программы - это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы-шпионы, нежелательное рекламное ПО и различные формы вредоносных кодов.

- Вредоносное ПО;
- Рекламное ПО;
- Шпионское ПО.

Спам. Спам - это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится получателю, 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. 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.

Коммуникационные риски. Коммуникационные 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.

Киберпреследования. 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.

Интернет-опасности, связанные с психологическими особенностями личности при использовании Интернета

Азартные игры в Интернете. Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. Сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

Онлайновое пиратство. Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом –например, музыки, фильмов, игр или программ – без разрешенияправообладателя.

Раскрытие личных данных. Последние исследованияпоказывают, что сегодня примерно половина всех веб-журналовпринадлежат подросткам. При этом двое из трех раскрывают свойвозраст; трое из пяти публикуют сведения о месте проживания иконтактную информацию, а каждый пятый сообщает свое полноеимя. Подробное раскрытие личных данных потенциально опасно.

Интернет-мошенничество и хищение данных кредитнойкарты. Интернет-мошенничество может осуществляться с помощью фальшивых электронных писем, в которые включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что оннаходится на официальном узле, хакеры пытаются склонить егок вводу паролей, номеров кредитных карт и другой секретнойинформации, которая потом будет использована в ущербпользователю. Поэтому, посещая веб-сайты, нужно самостоятельнонабирать в обозревателе адрес веб-сайта и не пользоваться ссылкой, содержащейся в подозрительном электронном письме.

Неправильное формирование нравственных ценностей.В Интернете встречаются материалы нежелательного характера, к которым можно отнести материалы порнографического, агрессивного содержания, материалы суицидальной направленности, сектантские материалы, включающие ненормативную лексику. Существуют средства фильтрации нежелательного материала, но фильтры могут только помочь в блокировании только некоторых нежелательных материалов и решить полностью проблему не могут. Поэтому взрослым важно поддерживать доверительные отношения с детьми, чтобы они без колебаний обращались за советом и помощью.(***Подробные рекомендации по обеспечению «технической безопасности» смотрите в разделе 4 данных методических рекомендаций***).

Советы родителям по предотвращению интернет-опасностей

1. ***Поговорите с вашими детьми.*** Вы должны знать, какие сайты они посещают, с кем общаются, что любят смотреть. Точно так же как вы не позволяете уходить из дома, не предупредив вас, куда и с кем ребенок пошел, вы не должны разрешать ему пользоваться интернетом, как ему захочется.
2. ***Установите правила для использования интернета.*** Четко определите время, которое Ваш ребенок может проводить в Интернете, и сайты, которые он может посещать. Контролируйте выполнение этих правил, особенно, если компьютер находится в комнате ребенка.
3. ***Запретите детям распространять личную информацию.*** Объясните ребенку, что опасно разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, номер школы и т.д.), а также «показывать» свои фотографии. Объясните ребенку, что при общении в Интернете на чатах, форумах и в других ситуациях, требующих регистрации, нельзя использовать реальное имя. Помогите ему выбрать регистрационное имя (ник), не содержащее никакой личной информации, вместо фотографии выберите аватар.

4. ***Научите детей быть осторожными.*** Расскажите ребенку о возможных опасностях Сети и их возможных последствиях. Ребенок должен знать, что нельзя открывать подозрительные файлы и ссылки, как бы заманчиво они не выглядели. Приучите ребенка спрашивать о том, в чем он не уверен.
5. ***Не позволяйте Вашему ребенку встречаться с on-line знакомыми.*** Объясните ребенку, что никогда нельзя быть уверенным в том, кто с тобой общается.
6. ***Научитесь сами, безопасно использовать интернет, чтобы затем советовать детям.*** Для многих родителей интернет является все еще неизвестным миром. Поэтому нам очень важно знать о том, что интернет предлагает нашим детям, чтобы затем советовать, как безопасно использовать интернет.
7. ***Контролируйте деятельность ребенка в Интернете*** с помощью специального программного обеспечения. (***Подробные рекомендации по обеспечению «технической безопасности» смотрите в разделе 4 данных методических рекомендаций***).

В разделе 5 представлена памятка учащимся при пользовании Интернет. С более подробной информацией об опасностях и правилахбезопасности в Интернете можно познакомиться в буклете http://www.ifap.ru/library/book099.pdf

Помимо Интернет-опасностей, связанных с психологическими особенностями личности, при использовании интернета существует еще и прямая угроза здоровью детей. Представим основные признаки возникновения информационной угрозы по физиологическим показателям ребенка.В **Таблице 1**представим основные негативные последствия, которые оказываются на организм ребенка во время работы с компьютером.

Таблица 1

Симптомы и показатели психического и физического здоровья человека, проявление которых свидетельствует о нарушении правил информационной безопасности

Негативные последствия	**Показатели, которые свидетельствуют о нарушении правил информационной безопасности**	**Симптомы и Механизмы воздействия на организм**
Вредные излучения при работе за компьютером воздействуют на здоровье	1. ЭЛТ (электронно-лучевая трубка) монитора создает ионизирующее(рентгеновское)излучение. 2.Электромагнитное излучение. 3.Электростатическое поле.	Электростатическое поле способствует оседанию пыли и аэрозольных частиц на лице, шее, руках, что может вызвать у людей негативные кожные реакции – сухость, аллергию. Влияет на ионный состав воздуха. На поверхности кинескопа монитора возникает положительный заряд, который нейтрализует отрицательно заряженные полезные ионы воздуха, что ухудшает среду в помещении с компьютером.
Компьютерные игры тормозят развитие лобных долей мозга	– нефиксированное время, проводимое за компьютером; – неустойчивое эмоциональное состояние	– нарушается способность к обучению (познавательная деятельность, память, абстрактное мышление) – нарушается способность формировать цели и задачи, а также планировать действия по достижению этих целей – ослабевает контроль своих действий и эмоциональных проявлений
Компьютер и **зрение**	Уже в первые годы компьютеризации было отмечено специфическое зрительное утомление у пользователей дисплеев, получившее общее название “компьютерный зрительный синдром”(CVS-computervisionsyndrome).	Признаки CVS: • Снижение остроты зрения • Замедленнаяперефокусировка с ближних предметов на дальние • Двоение предметов • Быстрая утомляемость при чтении • Чувство жжения в глазах • Ощущение “песка” под веками • Покраснение глаз • Боли в области глазниц и лба при

		движении глаз
Заболевания мышц и суставов Синдром длительной статической нагрузки **нарушение осанки**	• боли в руках • боли в шее • боли в пояснице Синдром канала запястья • дрожь • зуд • покалывание в пальцах	Симптом - **"рука, держащая мышь":** При работе за компьютером руки бывают постоянно согнуты в локтях, кисти в напряжении висят над клавиатурой. Кисть долго неподвижна и напряжена, кровообращение в ней застаивается и снабжение тканей кислородом замедляется. Происходит отек, сжимается нерв. В результате появляется боль, особенно ночью и рано утром, в пальцах ощущается покалывание или онемение Статичная искривленная поза быстро наносит ущерб - боли в спине, сколиоз, сутулость. Обратите внимание на осанку… На кисти рук…
Проблемы в социализации и адаптации	Игровая потребность - войти в роль компьютерного персонажа, обрести свое «виртуальное Я». «Я виртуальное» не испытывает проблем адаптации - оно сильное, умное, ловкое, ему доступно оружие, деньги, на которые можно купить все в виртуальном мире.	•разрушение целостной картины мира, •разорванность восприятия окружающей действительности, •ощущение жизни, как компьютерной игры в которой все можно многократно начать заново. •Реальный мир скучен, неинтересен и полон опасностей. •Компьютер становится мощным стимулом и главным объектом для общения. •Уменьшается круг общения ребенка и, как следствие, отсутствие жизненного опыта. •Человек замыкается в себе, снижает до минимума общение с реальным окружающим миром, становится холодным и равнодушным

Детские психологи и окулисты рекомендуют следующий режим работы на компьютере и организации рабочего места:

- 3 - 7 лет - не более 15 минут в сутки. Один день в неделю желательно компьютер не включать вовсе.
- 7 - 10 лет - от 15 до 30 минут. Правило одного дня без компьютера сохраняется.
- 10 - 14 лет - 1 час в сутки, желательно разбить сеанс на 2 раза.
- 14 - 17 лет - 1,5 - 2 часа в сутки с перерывами через каждые 20-30 минут.

Если у ребенка есть проблемы со зрением, необходимо разрешение детского врача – окулиста.

Помните! Норма времени за компьютером для каждой возрастной группы должна быть снижена ровно в два раза для ребенка, у которого наблюдаются проблемы со зрением.

Организация рабочего места

- Компьютер должен стоять в углу или задней стенкой должен быть обращен к поверхности стены.
- В комнате должно быть как естественное, так и искусственное освещение.
- Стол следует поставить сбоку от окна так, чтобы свет падал слева.
- Искусственное же освещение должно быть общим и равномерным, однако использование одних только настольных ламп недопустимо.
- Необходимо проветривать помещение, в котором работает компьютер.
- Необходимо ежедневно проводить тщательную влажную уборку.
- Необходимо протирать экран специальной салфеткой для удаления пыли.
- В процессе работы необходимо постоянно следить за положением тела.
- Голову следует держать ровно по отношению к плечам.

ПОВЫШЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ ДЕТЕЙ В ИНТЕРНЕТЕ ПРИ ПОМОЩИ ТЕХНИЧЕСКИХ И ТЕХНОЛОГИЧЕСКИХ СРЕДСТВ

Условно разделим инструментарий, который можно использовать для обеспечения ин-формационной безопасности в различных операционных системах (Windows и Linux) (рассматриваются только бесплатные версии), на несколько категорий:

1) Специализированное программное обеспечение для контентной фильтрации;
2) Функционал программ «Родительский контроль» или «Семейная безопасность»;
3) Специализированные детские браузеры;
4) Онлайн - сервисы для организации контентной фильтрации.
5) Рассмотрим каждый из инструментов более подробно.

Использование специализированных программ

1. Контент-фильтр «Интернет Цензор»http://icensor.ru/устанавливается как самостоятельная программа на компьютер и обеспечивает фильтрацию для всех веб-браузеров и программ. Программа «Интернет Цензор Лайт» устанавливается как дополнение к веб-браузеру MozillaFirefox и обеспечивает фильтрацию только для данного браузера. Программа «Интернет Цензор» проста в установке и использовании. Отличительной особенностью полной версии является высокий уровень защищённости от попыток ребёнка обойти фильтрацию или взломать программу.
2. ChildProtecthttp://cp.s-soft.org/это социальный проект, цель которого оградить детей от нежелательного содержимого в Интернет. При попытке осуществить доступ на порносайт, который имеется в базе, браузер будет выдавать ошибку "Сервер не найден". У ребенка будет создаваться ощущение, что такого сайта не существует.
3. Программа K-9 http://www1.k9webprotection.com/ предназначена для эффективной защиты компьютеров, на которых работают дети, от аморального, запрещѐнного или травмирующего психику контента.
4. NaomiInternetFilter фильтр Интернет-контента http://www.newestsoft.com/Windows/Web-Development/Wizards-Components/Naomi-3290.html. При своей работе утилита контролирует содержимое, загружаемое из интернета, и запрещает доступ к различным порносайтам, а также сайтам, содержащим насилие и пропаганду терроризма, азартные игры и т.д.
5. Дополнение AdblocksPlus к браузеру MozillaFireFox. Это мультиплатформенное решение позволяет настроить контент - фильтрацию и дополнительно избавиться от надоедливой рекламы и всплывающих окон на сайтах.
6. Программа KontrolLitehttp://www.kontrol.info/бесплатная версия Интернет-фильтра семейства Kontrol, которая позволяет блокировать порносайты. Отключить ее могут только родители
7. NetPoliceLitehttp://netpolice.ru/filters/lite/ – упрощенная версия платной программы NetPolice. К основным возможностям упрощѐнной версии относятся: регулярные информационные отчеты, 5
категорий фильтрации, доступ к настройкам по единому паролю, перенаправление на безопасный поисковик и др.
8. HandyCachehttp://handycache.ru/ - это программа, которая экономит трафик, ускоряет загрузку страниц, блокирует рекламу и иное нежелательное содержимое и позволяет в автономном режиме (без подключения к Интернет) просмотреть любые посещенные ранее сайты.
9. ParentalControlhttp://www.securitylab.ru/software/270756.php – дополнение к браузеру InternetExplorer, которое помогает предотвратить доступ детей к сайтам для взрослых.
10. Межсетевой фильтр Iptables(Для операционных систем, серверов на базе Linux) обладает весьма широкими возможностями по настройке безопасности, что значительно усложняет его практическое освоение детьми.
11. Прокси-сервер Squid (Для операционных систем, серверов на базе Linux) является удобным инструментом для организации контентной фильтрации.

Использование функции «родительского контроля» или «семейной безопасности» на компьютерах, с которыми работают школьники

1. Семейная безопасность WindowsLive 2011 для ОС Vista и 7 http://explore.live.com/windows-live-family-safety?os=winxp.
2. Для Windows XP – http://explore.live.com/windows-live-family-safety-xpустанавливайте ограничения на поисковые запросы, отслеживайте посещаемые сайты, разрешайте или блокируйте доступ к ним.
3. Если на компьютере используются антивирусная программа KasperskyInternetSecurity версии 2010, то в этой программе есть вкладка «Родительский контроль», где можно заблокировать доступ к нежелательным сайтам.

Использование специализированного браузера, созданного для детской аудитории

Детский браузер Гогульhttp://www.gogul.tv/специально разработанный для детей, их родителей и воспитателей. Эта программа мультиплатформенная, т.е. работает и в Linux и в среде Windows.

Использование виртуальных социальных сервисов по осуществлению контентной фильтрации с ведением «белых списков» сайтов, специально организованных для работы с детьми

1. http://school.yandex.ru/ - Это проект школьный Яндекс.
2. NetPolice DNS http://netpolice.ru/filters/dnsfilter/ поможет Вам ограничить доступ к нежелательному содержимому.
3. Портал «ТЫРНЕТ – Детский Интернет» http://www.tirnet.ru-Этот сервис включает в себя услугу «прокси», которая не позволит ребенку по баннерам и гиперссылкам перейти на нежелательные ресурсы.

Программы фильтрации «Обзор программ» и ссылки на сайты разработчиков можно посмотреть на сайте Лиги безопасного интернета www.ligainternet.ru.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

Решение задачи по обеспечению безопасности прииспользовании компьютера и Интернета детьми требуеткомплексного подхода, решения множества психолого-педагогических вопросов. Помимо выполнения очевидных мербезопасности (установка антивирусных программ, брандмауэров,фильтров, ограничений по времени) необходима разработка иреализация правил электронной безопасности, которые требуютпривлечения широкого круга заинтересованных лиц: директорашколы, классных руководителей, преподавателей информационныхтехнологий, самих учащихся и их родителей,поставщиков услугИнтернета. Информационная безопасность в Интернете можетобсуждаться во время уроков информатики, социологии, ОБЖ,гражданского права и др.

Комплексное решение поставленной задачи со стороны семьи и школы позволит значительно сократить риски причинения различного рода ущерба ребенку со стороны сети Интернет. Обеспечение информационной безопасности и воспитание информационной культуры должно стать приоритетным направлением работы современного образовательного учреждения.

В приложении 2 представлено примерное планирование работы школы по обеспечению информационной безопасности учащихся.

Путь решения этой проблемы может быть обозначен словамиН.Е. Щурковой: «Специфика педагогической работы с детьмисостоит не в том, чтобы подавить негативные проявления личности,

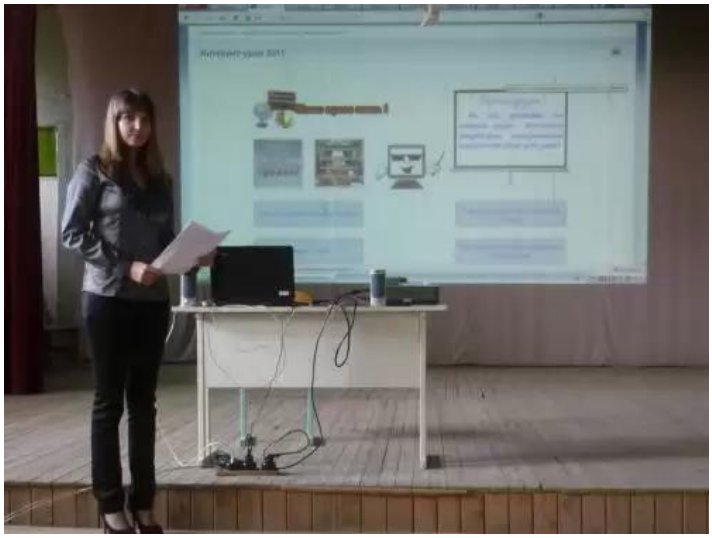
а в том, чтобы, не обедняя ни содержательно, ни методически воспитательного процесса, осуществить необходимое для каждого ребенка на земле вхождение в контекст высоких современных достижений культуры; сохраняя достоинство личности, перевести её поведение на уровень культуры».

Ограничение доступа к нежелательной информации нужносочетать с демонстрацией качественных образовательныхресурсов. Поэтому изучение разделов школьной программынеобходимо снабдить ссылками как на традиционные бумажные,так и электронные учебники, учебные пособия, энциклопедии,справочники, словари, ресурсы электронных федеральныхобразовательных коллекций, цифровых хранилищ библиотеки музеев, образовательных сайтов, дидактические материалыучителя, работы других учащихся. Задача информационнойдеятельности учителя и ученика на этой стадии заключается всовместном расширении и систематизации сети используемыхинформационных образовательных источников. При переходеиз класса в класс количество используемых образовательныхресурсов неизбежно увеличивается.

Если в первом классе ученик преимущественно пользуется учебником и рабочей тетрадью, то перед одиннадцатиклассником открывается бескрайний океан мировых информационных ресурсов накопленных за всю историю цивилизации. Ограничение в доступе к этим ресурсам, ведет «к цифровому неравенству между людьми».

Учитель ориентирует учащихся в доступных информационных образовательных ресурсах по теме урока, проекта, учащиеся самоопределяются в выборе информационных источников. При необходимости учащиеся осуществляют самостоятельный поиск информации по ключевым словам темы в сети с использоанием поисковых систем Интернет, работают с коллективными закладками, совместно создают гиперссылки на образовательные ресурсы; составляют каталог ресурсов по теме, размышляют над рефлексивными вопросами об информационных ресурсах темы. В качестве примера учащимся может быть предложен список ресурсов расположенный на страницах сайта Центра информационных технологий в обучении «Познание»: https://sites.google.com/site/poznanietime/resources. Так же современные электронные учебные модули, размещенны на сайте Федерального центра информационно-образовательных ресурсов: http://fcior.edu.ru/ и в Единой коллекции цифровых образовательных ресурсов: http://school-collection.edu.ru/.

Учитель организует поиск дополнительных источниковчерез библиотечные каталоги, поисковые системы Интернет,учит отбирать и систематизировать их. В работах Е.С. Полат,указывается на то, что необходимо обращать внимание учащихся на объективность и надежность предлагаемой информации: ее источник, автора публикации, принадлежность источника к определенной культурной, политической, конфессиональной среде. Кроме того, необходимо учить подростков анализировать информацию с позиции общечеловеческих ценностей; отделять факты от субъективных мнений; отделять эмоции от фактов; рассматривать проблему с разных сторон, а не только с позиции автора; устанавливать взаимосвязь явлений; связывать разнородные объекты; объединять противоположности, стараясь найти дополнительные аспекты рассмотрения проблемы; обобщать полученную информацию и делать выводы, принимать решения; оценивать полученную информацию по совокупности проведенного анализа; прогнозировать последствия при-нятого решения. Этим базовым умениям безопасной работы с информацией необхо-димо обучать школьников в процессе познавательной деятельности по любому предмету школьнойпрограммы.



Участвуя в информационной дея-тельности, подростки не только ищут, ана-лизируют, используют готовые ресурсы, но и создают собственные информационные продукты: аннотации, сообщения, доклады и др., в том числе с использованием ИКТ: мультимедийные презентации, публикации, таблицы, диаграммы, а также карты памяти, вики-статьи, электронные каталоги, гипер-медийные тексты, делятся ссылками на созданные ресурсы.

Для обучения ребенка информаци-онной безопасности необходимо предусмотреть решение типовых ситуаций информационных угроз, которое представляет определенный **алгоритм поведения в конкретной ситуации информа-ционной угрозы** (рис.1). Каждый учащийся должен овладеть данным алгоритмом на уровне навыка, привычки, чтобы в экстремальной ситуации информационной угрозы принять единственно верное решение и сохранить свою безопасность.

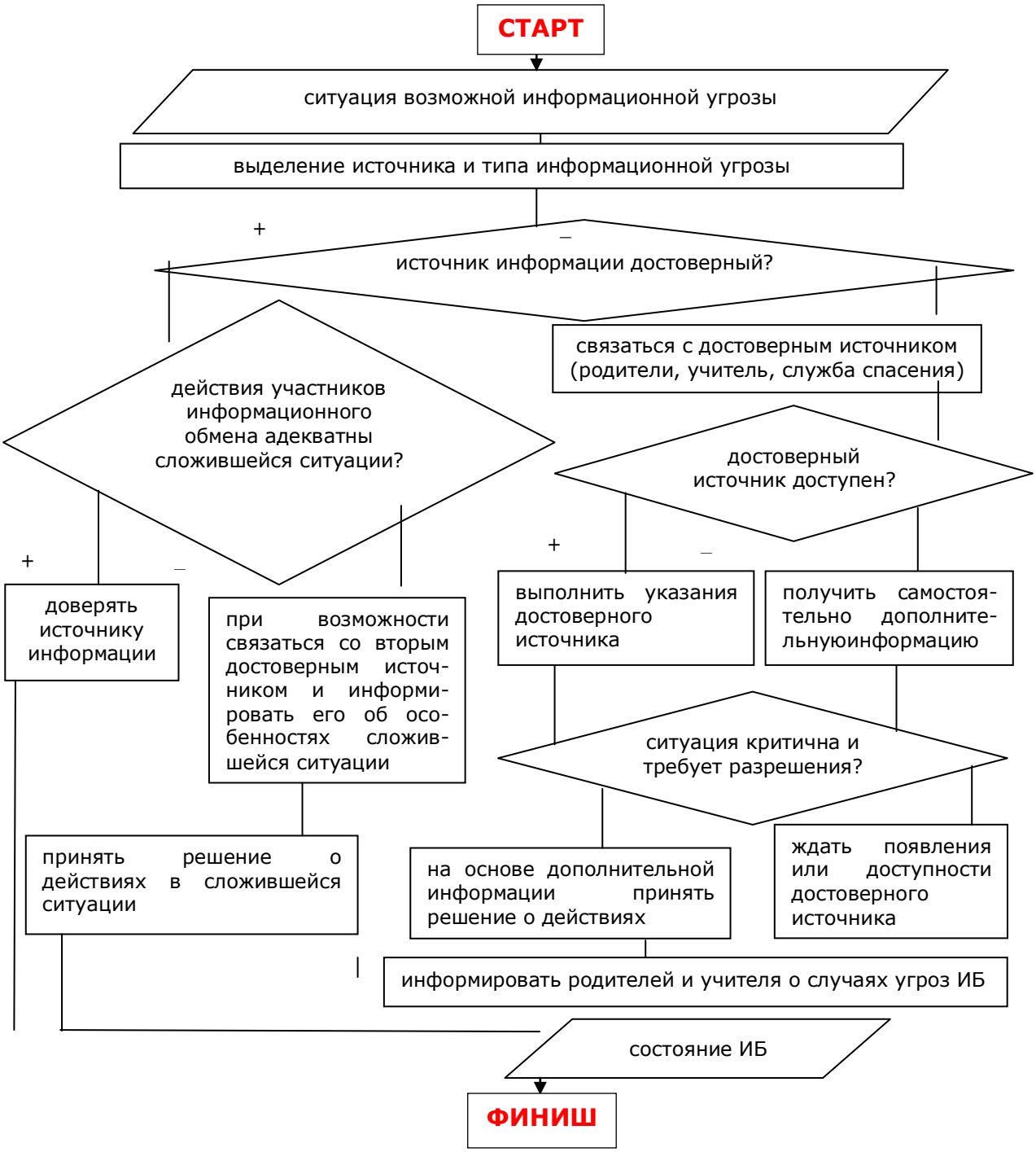


Рис.1. Алгоритм поведения ребенка в ситуации информационной угрозы

Основу обучения информационной безопасности школьников составляют базовые умения работы с информацией для формирования которых необходимо:

1) развить критическое мышление ребенка (уметь анализировать ситуацию, имеющуюся информацию, сопоставлять ее с ранее известной, делать выводы, сравнивать, обобщать);
2) научить выделять источник информации в сложившейся ситуации;
3) дать представления о различных видах предлагаемой информации: недостоверной, неэтичной, деструктивной;
4) научить определять информационную угрозу, понимать возможность ее негативного воздействия (вред здоровью, межличностному общению);
5) научить принимать единственно правильное решение в зависимости от сложившейся ситуации (позвонить по нужному номеру телефона, сказать взрослым и др.).

Для примера рассмотрим алгоритм поведения ребенка в ситуации информационной угрозы «Предлагаю дружбу»: ребенок один за компьютером в сети Интернет, по электронной почте приходит сообщение под названием «Давай дружить».

На первом этапе возникшей ситуации угрозы нужно по возможности, не обнаруживая себя и не сообщая о себе (особенно о том, что ребенок находится один) никакой информации, получить как можно больше сведений. В данном случае – разместитьданные автора сообщения в раздел «Поиск».

Прежде всего ребенку необходимо дать объективную оценку предлагаемой информации, удостовериться в ее истинности и надежности и в соответствии с полученным результатом принять единственно правильное решение, которое поможет сохранить жизнь и избежать риска быть обманутым недобросовестными людьми. Для анализа информации важно понять: от когои в какое время она поступила.

Таким образом, проблема информационной безопасности детей сегодня стоит очень остро, мы попытались выработать алгоритм поведения ребенка в ситуации информационной угрозы. Также следует обратить внимание, что именно родители в ответе за безопасность детей, поэтому необходимо повышать родительскую компетентность в этом вопросе.

Достичь высоких результатов в воспитании и обеспечении информационной безопасности невозможно без привлечения родителей. Очень часто родители не понимают и недооценивают угрозы, которым подвергается школьник, находящийся в сети Интернет. Некоторые из них считают, что ненормированное «сидение» ребенка в сети лучше, чем прогулки в сомнительных компаниях. Родители, с ранних лет обучая ребенка основам безопасности дома и на улице, между тем «выпуская» его в Интернет, не представляют себе, что точно также нужно обучить его основам безопасности в сети. Ребенок абсолютно беззащитен перед потоком информации, сваливающейся на него из сети.

С родителями необходимо вести постоянную разъяснительную работу, т.к. без понимания родителями данной проблемы невозможно ее устранить силами только образовательного учреждения. Формы работы с родителями могут быть разнообразны: выступления на родительскихсобраниях, индивидуальные беседы, информация на сайте школы, встречи со специалистами, семинарские занятия. Должны быть разработаны специальные методические рекомендации для родителей по обеспечению информационной безопасности в Интернет. Они должны содержать классификацию Интернет угроз, рекомендации по обеспечению безопасности ребенка в Интернет дома (в зоне ответственности родителей).

В приложении 4 представленыформы работы с родителями при организации всеобуча для родителей по обеспечению информационной безопасности детей и подростков (из опыта работыобразовательных учреждений Тюменской области).

Формы разъяснения правил информационной безопасности могут быть представлены в различных вариантах, в зависимости от аудитории с которой происходит работа. **Ниже предложена полезная информация, которая может быть включена в любые мероприятия с детьми и работу с родителями.**