Методические рекомендации

по безопасному использованию Интернета детьми

Проблема обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

Интернет имеет очень большое количество возможностей, которые в наше время широко используются. К ним относятся поиск информации, заработок в интернете, получение образования с использованием дистанционных форм обучения, развлекательные ресурсы, общение в реальном времени и т.д. В сети Интернет существует и вредоносные возможности, одним из них являются компьютерные вирусы. Каждый пользователь знает о компьютерных вирусах. Многие сталкивались с ними, занимались лечением своего компьютера от вирусов. Но у многих сообщение о том, что их компьютер заражен вирусами, вызывает реакцию «Все пропало!».

Использование сети Интернет в нашей школе направлено на решение задач образовательного процесса. Для этого используются два компьютерных класса, подключенных к сети Интернет, автоматизированные рабочие места педагогов. На всех компьютерах установлено лицензионное или свободно-распространяемое программное обеспечение.

Существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для детей угрозу.

Какие же опасности ждут школьника в сети Интернет? Прежде всего можно выделить следующие:

- суицид-сайты, на которых дети получают информацию о «способах»расстаться с жизнью;
- сайты-форумы потенциальных самоубийц;
- наркосайты. Интернет пестрит новостями о "пользе” употребления марихуаны, рецептами и советами изготовления "зелья”;
- сайты, разжигающие национальную рознь и расовое неприятие: экстремизм, национализм, фашизм;
- сайты порнографической направленности;
- сайты знакомств. Виртуальное общение разрушает способность к общению реальному, "убивает” коммуникативные навыки подростка;
- секты. Виртуальный собеседник не схватит за руку, но ему вполне по силам "проникнуть в мысли” и повлиять на взгляды на мир.

Социальные сети, такие как Одноклассники, Вконтакте, MySpace, Facebook, Twitter и многие другие позволяют людям общаться друг с другом и обмениваться различными данными, например, фотографиями, видео и сообщениями. По мере роста популярности таких сайтов растут и риски, связанные с их использованием.

Для ограничения доступа к сайтам, не совместимыми с задачами образования, на компьютерах установлен фильтр Интернет-Цензор.

Методическим советом школы разработаны рекомендации для обучающихся и их родителей по безопасному использованию ресурсов сети Интернет .

Эти советы помогут защитить персональные данные при работе с социальными сетями.

- **Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях от других пользователей или друзей.** Не следует бездумно открывать все ссылки подряд - сначала необходимо убедиться в том, что присланная вам ссылка ведет на безопасный или знакомый вам ресурс
- **Контролируйте информацию о себе, которую вы размещаете.** Обычно злоумышленники взламывают учетные записи на сайтах следующим образом: они нажимают на ссылку "Забыли пароль?" на странице входа в учетную запись. При этом для восстановления или установки нового пароля, система может предлагать ответить на секретный вопрос. Это может быть дата вашего рождения, родной город, девичья фамилия матери и т.п. Ответы на подобные вопросы можно легко найти в сведениях, которые вы опубликовали на своей странице в какой-либо популярной социальной сети. Поэтому при установке секретных вопросов необходимо придумывать их самостоятельно (если сайт, на котором вы регистрируетесь, это позволяет) или старайтесь не использовать личные сведения, которые легко найти в сети.
- **Не думайте, что сообщение, которое вы получили, было отправлено тем, кого вы знаете, только потому, что так написано.** Помните, что хакеры могут взламывать учетные записи и рассылать электронные сообщения, которые будут выглядеть так, как будто они были отправлены вашими друзьями. Если у вас возникло такое подозрение, будет лучше связаться с отправителем альтернативным способом, например, по телефону, чтобы убедиться в том, что именно этот человек отправил вам данное сообщение. Точно также необходимо относиться и к приглашениям зарегистрироваться в той или иной социальной сети.
- **Чтобы не раскрыть адреса электронной почты своих друзей, не разрешайте социальным сетям сканировать адресную книгу вашего ящика электронной почты.** При подключении к новой социальной сети вы можете получить предложение ввести адрес электронной почты и пароль, чтобы узнать, есть ли в этой сети пользователи, с которыми вы уже поддерживаете отношения при помощи электронной переписки. Используя эти данные, сайт может рассылать электронные сообщения (например, приглашения присоединиться к этой сети от вашего лица) всем пользователям из вашего списка контактов. Социальные сети должны указывать то, что эти адреса электронной почты будут использованы для этой данной, но зачастую не делают этого.
- **Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки.** Нажав на ссылку, которую вы получили в электронном сообщении или нашли на каком-либо сайте, вы можете попасть на

поддельный сайт, где оставленные вами личные сведения будут украдены мошенниками.

- **Не добавляйте в друзья в социальных сетях всех подряд.** Мошенники могут создавать фальшивые профили, чтобы получить от вас информацию, которая доступна только вашим друзьям.
- **Не регистрируйтесь во всех социальных сетях без разбора.** Оцените сайт, который вы планируете использовать, и убедитесь, что вы правильно понимаете его политику конфиденциальности. Узнайте, существует ли на сайте контроль контента, который публикуется его пользователями. К сайтам, на которых вы оставляете свои персональные данные, необходимо относиться с той же серьезностью, которой требуют сайты, где вы совершаете какие-либо покупки при помощи кредитной карты.
- **Учитывайте тот факт, что все данные, опубликованные вами в социальной сети, могут быть кем-то сохранены.** На большинстве сервисов вы можете в любой момент удалить свою учетную запись, но, не смотря на это, не забывайте, что практически любой пользователь может распечатать или сохранить на своем компьютере фотографии, видео, контактные данные и другие оставленные вами сведения.
- **Проявляйте осторожность при установке приложений или дополнений для социальных сетей.**Многие социальные сети позволяют загружать сторонние приложения, которые расширяют возможности личной страницы. Довольно часто такие приложения используются для кражи личных данных, поэтому к их использованию необходимо относиться также серьёзно, как и к установке на свой компьютер программ, которые вы можете найти в Интернете.

1. Советы для родителей

1. Поговорите с Вашими детьми. Вы должны знать, какие сайты они посещают, с кем они общаются, что они любят смотреть и т.д.

2. Обучите себя и поделитесь этими знаниями с Вашими детьми. Очень важно знать о тех утилитах, которые Интернет предлагает детям, о рисках, которые они могут в себе нести, а также о том, как их можно избежать.

3.Установите правила для использования Интернета. Вы должны установить четкие и понятные правила, которые описывают расписание выхода в Интернет, максимальную продолжительность работы в Интернете, а также способ его использования. И убедитесь, что Ваши дети следуют этим правилам.

4. Запретите детям предоставлять конфиденциальную информацию. Вы должны проинструктировать Ваших детей о том, что им нельзя предоставлять кому-либо в Интернете такие данные, как свои имя, адрес или фотографии.

5. Научите своих детей быть осторожными. Зачастую в Интернете многие вещи выглядят не так, как они нам представляются. Научите Ваших детей быть осторожными и приучите их не делать ничего такого, что могло бы поставить под угрозу их безопасность и конфиденциальность.

Для учащихся 9 класса разработан и будет реализован во втором полугодии 2014-2015 учебного года интегрированный элективный курс «Государство и гражданин в современном Интернет - пространстве», целями и задачами которого являются : умение вести себя в ситуации, когда надо получить ту или иную госуслугу, пользоваться сервисами государственных организаций, Портала, применять Интернет для поиска и получения информации по госуслугам, умение работать с документами, позволяет школьникам использовать полученные знания на практике.

При правильном использовании ресурсов сети Интернет можно добиться положительных результатов в работе школы, а применение **Интернета** непосредственно на уроке повышает уровень информационной культуры ученика. Так как Интернет и Школа — реальный путь к успеху.

1. Методические рекомендации по проведению уроков «Безопасность в Интернете» в общеобразовательных учреждениях http://www.safe-internet.ru/competition/guidelines.pdf
2. Портал Сети творческих учителей. http://www.it-n.ru/communities.aspx?cat_no=71586&tmpl=com
3. Майкрософт – центр безопасности http://www.microsoft.com/ru-ru/security/online-privacy/social-networking.aspx
4. Ребенок в сети http://www.detionline.ru/advise.htm