**[ИНСТРУКЦИЯ](https://us-school11.ru/wp-content/uploads/2015/02/instrukciya.doc)**для педагогических работников школы о порядке действий при осуществлении контроля использования обучающимися сети Интернет

Проблема информационной безопасности образовательного учреждения превращается в последнее время из гипотетической во вполне реальную. Количество угроз растет с каждым днем, изменяется нормативно-правовая база, соответственно реалиям времени должны изменяться и методы обеспечения информационной безопасности учебного процесса.

В современной школе информация, информационная инфраструктура – один из главных компонентов учебного процесса. Учебные классы оснащаются компьютерной техникой и её качественное бесперебойное функционирование существенно определяет качество полученных знаний, способствует формированию профессиональных компетенций учащихся.

Вот поэтому-то обеспечение информационной безопасности учебного процесса, в том числе непрерывного функционирования компьютерных и информационных ресурсов, является весьма важной для его качества.

**Принятые меры по созданию безопасной информационной системы в школе**  
•    Обеспечена защита компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, логические бомбы, атаки хакеров и т. д.)•    Установлен строгий контроль за электронной почтой, обеспечен постоянный контроль за входящей и исходящей корреспонденцией.  
•    Установлены соответствующие пароли на персональные ЭВМ  
•    Использованы контент-фильтры  для фильтрации сайтов по их содержимому.

**Нормативно-правовая база определяющая порядок защиты информации:**  
**•    Ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях по защите информации»**  
•    Ст. 9 Закона № 149-ФЗ, п. 5 — информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей подлежит защите в случаях предусмотренных законом (государственная тайна)  
•    Гл. 14 Трудового кодекса РФ (далее – ТК РФ) — защита персональных данных работника.  
•    Федеральный закон № 152-ФЗ РФ «О персональных данных», который вступил в силу с 1 января 2008 г. — обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных.

**Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) «О защите детей от информации, причиняющей вред их здоровью и развитию»**

**Родительский контроль**

    Родительский контроль — это ограничение доступа детей и подростков к нежелательным сайтам в Интернет, например, порносайтам, пропаганде насилия, сайтам знакомств, игровым сайтам, социальным сетям и т.д. Родительский контроль может не только блокировать доступ к нежелательным для детей сайтам, но ограничивать использование Интернет по времени суток, днямнедели илидлительности сеанса. Существует множество программ и фильтров, которые помогут вам контролировать открытие нежелательной информации и время, которое можно проводить в Интернете. Вы можете воспользоваться одной из ниже перечисленны

**Антивирус Касперского с возможностями Родительского контроля — «Kaspersky Internet Security»,**

**программа-фильтр «NetPolice»,**

**программа-фильтр «Интернет Цензор».**

**Рекомендации для родителей**

Как уже отмечалось ранее, в большей степени от Вас, чем от кого-либо другого, будет зависеть, повлияют ли негативно или позитивно различные средства массовой информации, Интернет, видео и аудио на развитие вашего ребенка. Это было доказано проведенным исследованием, через научный анализ полученных результатов опроса. По результатам исследования видно, что чем больше родитель уделяет внимания своему ребенку, тем меньше риск негативного влияния негативной информации, которую ребенок получает через телевидение, интернет, музыку, которую он слушает и др. источники. Это внимание заключается:- в контроле того, что ребенок делает и что смотрит; Контроль не должен быть агрессивным, Вы не должны всем своим видом показывать, что это КОНТРОЛЬ. Такой метод вызовет у ребенка негативную реакцию и может привести к обратным результатам. Контролировать необходимо: — время, которое ребенок проводит за компьютером или телевизором или др. По результатам различных исследований видно, что ребенок, имеющий какие-либо увлечения, который ходит в различные секции, кружки, имеет меньше вредных привычек, ведет более здоровый образ жизни и он меньше подвержен воздействию негативной информации. Поэтому постарайтесь организовать досуг ребенка. Первоначально понаблюдайте за ним, выявите его интересы, затем вовлеките ребенка в кружки или секции, которые соответствуют его интересам. Зачастую, прежде чем выбрать свое увлечение, ребенок меняет несколько кружков, но потом на чем-то останавливается. Есть платные кружки и секции, но есть и бесплатные при школе. Если у вас в школе нет секций и кружков, то свяжитесь с родительским комитетом школы, с директором, и Вы можете помочь школе открыть такой кружок. Обезопасить ребенка от негативного влияния СМИ, Интернет, аудио — и видеопродукции очень сложно в одиночку, работа должна проходить комплексно, с участием различных сторон, окружающих ребенка. Поэтому в этом Вам может помочь в первую очередь школа. Не стесняйтесь обращаться за помощью к социальному педагогу, классному руководителю и другим. Школа, со своей стороны, будет проводить работу по обеспечению информационной безопасности детей, но ей будет легче, если родители сами будут проявлять инициативу. При опросе детей в рамках данного исследования, у них выяснялись рекомендации по профилактике негативного воздействия современных информационных технологий на развитие ребенка. И вот какие рекомендации свои родителям они дали:

1) Заблокируйте каналы, несущие негативную информацию.

2) Ежедневно просматривайте «историю» в интернете.

3) Проверьте круг общения ребенка.

Данные рекомендации были составлены на основе информации, размещенной на сайтах различных IT-компаний и образовательных сайтах. Также были включены рекомендации школьных учителей информатики. Поэтому родители и педагоги сначала сами должны научиться азам информационной безопасности, а потом научить этому своих детей.

«Угроза заражения вредоносным программным обеспечением (ПО). Ведь для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.

Контакты с незнакомыми людьми с помощью чатов или электронной почты. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи; Вы не можете просто запретить своему ребенку посещать Интернет, так как, во-первых, он должен развиваться «в ногу со временем» и не должен отставать в развитии от своих сверстников, во-вторых, он все равно будет посещать интернет-сайты, но только без Вашего ведома, что еще больше увеличит угрозу. Поэтому мы предлагаем некоторые рекомендации, которые, возможно, помогут Вам защитить своего ребенка:

* Объясните детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством.
* Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т. д.
* Научите ваших детей уважать собеседников в Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни.
* Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернет – правда. Приучите их спрашивать о том, в чем они не уверены.
* Регулярно проверяйте список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются.
* Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.
* Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.
* Детям до 10 лет рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку.
* Покажите ребенку, что вы наблюдаете за ним не только потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
* Периодически, а лучше ежедневно проверяйте отчеты, на какие сайты заходил Ваш ребенок. Это можно сделать через Родительский контроль (см. далее) или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе Windows Vista).
* Внимательно проверяйте запросы на включение в список новых друзей. Помните, что в Интернете человек может оказаться не тем, за кого он себя выдает.
* Не забывайте контролировать детей в Интернет с помощью специального программного обеспечения. Это поможет вам отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.
* Скажите им, что не стоит встречаться с друзьями из Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают.
* Объясните своему ребенку, что в реальной жизни и в Интернет нет разницы между неправильными и правильными поступками.
* Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т. д.), использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации.
* Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет.
* Неконтролируемые покупки. Эта угроза в настоящее время стала весьма актуальной»
* Доступ к нежелательному содержимому. Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики, порнография, страницы, подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна, содержащие любую информацию, чаще всего порнографического характера.
* *Итак, какие же угрозы содержит Интернет?*
* Итак, следует понимать, что подключаясь к Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Также следует помнить, что даже самые искушенные дети не видят опасностей Интернета и не осознают рисков его использования. Дело в том, что у детей еще не сформированы критерии различия, ребенку интересно все.
* Советы по обеспечению безопасности ребенка в Интернет
* Не допускайте сквернословия.
* Прячьте модемы, когда уходите по делам.
* Регулируйте просмотр детьми телевидения.
* По проведенным ранее исследованиям видно, что очень большое влияние на психологическое состояние ребенка оказывает семейное окружение. Для ребенка самое важное – это понимание со стороны родителей. Регулярно разговаривайте с ребенком, постарайтесь узнавать его проблемы, давайте ему советы как поступить в той или иной ситуации. Ни в коем случае не порицайте ребенка, если он открыл вам свой какой-то негативный поступок. Этим Вы можете его оттолкнуть, и в следующий раз он не расскажет вам свой секрет. Спокойно выслушайте его, постарайтесь понять, почему ребенок совершил тот или иной поступок, объясните ему, что вы его понимаете, но лучше так не поступать в следующий раз потому что….(объясните почему). Помните, что очень часто дети «замыкаются в себе», и как следствие «уходят в виртуальный мир» или попадают в плохую компанию, именно потому, что не видят интереса к себе со стороны близких людей и считают, что родители их не любят и не понимают. Если Вы не можете наладить «контакт» с ребенком, то можете обратиться за советом к школьному или другому психологу, так же сейчас есть много телевизионных передач, статей и книг о том, как улучшить взаимопонимание между родителем и подростком.
* В связи с тем, что в большей степени Интернет, чем другой какой-либо носитель информации притягивает внимание наших детей, и тем, что этот источник сложнее всего контролировать взрослым, то о том, как обеспечить безопасность вашего ребенка во Всемирной паутине поговорим отдельно и подробно.
* Постарайтесь вовлекать ребенка в какие-то совместные дела, но это не должна быть только уборка дома, стирка или другое полезное для дома мероприятие, вы можете вместе сходить в кино, смастерить что-либо, можете взять хороший фильм и его посмотреть, поиграть в какую-либо игру и т. д. В связи с тем, что у ребенка есть большой интерес к современным информационным носителям, то вы можете вместе поискать полезную информацию в интернете, заодно объясняя ребенку правила пользования этим средством.

- содержание того, что смотрит ребенок;

- в вовлечении ребенка в какие-то полезные для него занятия.

- в разъяснении ребенку, какая информация полезна для его развития, а какая может нанести вред;

* Всю работу по противодействию негативной информации необходимо начинать как можно с более раннего возраста ребенка. Если Вы не занимались с ребенком до 13-14 лет, а потом взялись за его воспитание, то результаты достичь будет намного сложнее, чем если бы Вы начали с 5-6 лет, а то и ранее. Поэтому Вы должны настроиться, что могут быть и неудачи, ребенок может сопротивляться вашему «вторжению» в его жизнь. Поэтому обучайте ребенка информационной грамоте как можно более деликатнее.
* Мы постараемся Вам помочь защитить вашего ребенка от негативного воздействия различных информационных технологий через ряд простых рекомендаций.

**ЭТО ВАЖНО!!!!!!!**

* Если у тебя возникли вопросы или проблемы при работе в онлайн-среде, обязательно расскажи об этом кому-нибудь, кому ты доверяешь. Твои родители или другие взрослые могут помочь или дать хороший совет о том, что тебе делать. Любую проблему можно решить! Ты можешь обратиться на линию помощи «Дети онлайн» по телефону: 88002500015 (по России звонок бесплатный) или
* **e-mail: .**

Специалисты посоветуют тебе, как поступить.