ПРИНЯТО
педагогическим советом
МКУДО ЦДТ
(протокол от 30.08.2018г. № 1)

СОГЛАСОВАНО
Управляющим советом
МКУДО ЦДТ
(протокол от 30.08.2018г. № 1)

УТВЕРЖДЕНО
приказом МКУДО ЦДТ
№ 45-Од от 30.08.2018г.

Положение
о защите учащихся МКУДО «Центр детского творчества» от воздействия негативной информации

1.Общие положения

1.1. Настоящее положение разработано в соответствии с Конституцией РФ, Законом Российской Федерации от 29 декабря 2012 года г. № 273 «Об образовании в Российской Федерации», "Об основных гарантиях прав ребёнка в Российской Федерации", Конвенциях о правах ребенка, Федеральный законом Российской Федерации от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

1.2. Информацией, оказывающей негативное влияние на детей, считается следующая информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
- отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера.

1.3. К информации, распространение которой среди детей ограничено, относится следующая информация:

- представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
- вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
- представляемая в виде изображения или описания половых отноше-

ний;

- содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

2.Цели противодействия негативному информационному воздействию

2.1. К целям противодействия негативному информационному воздействию относятся:

- выявление потенциальных и реальных источников негативного информационного воздействия на ребенка (печатные издания, Интернет ресурсы);
- обеспечение контентной фильтрации, способствующей ограничению доступа к интернет ресурсам, содержащим нелегальный и потенциально опасный контент;
- разработка специальных разработок, методических материалов, презентаций, посвященных тому, как обучать школьников правилам поведения в Интернете;
- просвещение родителей (законных представителей) обучающихся и воспитанников по использованию программ для родительского контроля детей в Интернете.

3.Требования к организации противодействия негативному информационному воздействию

3.1. Требования к организации противодействия негативному информационно-психологическому воздействию следующие: системность, активность, оперативность:

- системность - системный подход к организации противодействия негативному информационному воздействию;
- активность - стремление добиваться выполнения поставленных задач. Достигается: умелой организацией применения средств, проявлением инициативы;
- оперативность - своевременное блокирование каналов поступления негативной информации.

4.Обязанности педагога по обеспечению контроля над использованием учащимися сети Интернет

4.1. Во время занятий контроль над использованием учащимися сети Интернет осуществляет педагог дополнительного образования.

4.2. Педагог, ответственный за проведение занятия, выполняет следующие обязанности:

- определяет время и место для свободной работы учащихся в сети Интернет с учетом использования соответствующих технических возможностей в образовательном процессе, а также длительность сеанса работы одного учащегося;
- способствует осуществлению контроля за работой в сети Интернет,
- наблюдает за использованием компьютеров и сети Интернет учащимися;

- запрещает дальнейшую работу учащегося в сети Интернет в случае нарушения учащимся порядка использования сети Интернет и предъявляемых к учащимся требований при работе в сети Интернет; принимает необходимые меры для пресечения попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования, воспитания и развития.

Информация для родителей

«Как защитить ребенка
от негативного контента в СМИ и Интернет?»

Слово «контент» происходит от английского «content»- содержание. Контент - любой вид информации (текст, аудио, видео, изображение), составляющий содержание информационного продукта. Под «контентом» в широком смысле понимают наполнение сайта. В более узком смысле слова «контент сайта» - это материалы, размещенные на нем: в основном тексты, а также картинки и музыка. Вебсервисы контентом не являются. Самые характерные примеры контент-сайтов - интернет-СМИ и библиотеки, т.е. подборки текстов.

Развитие высоких технологий, открытость страны мировому сообществу привели к незащищенности детей от противоправного контента в информационно-телекоммуникационной сети «Интернет». По информации Генеральной прокуратуры Российской Федерации в 2012 году более 93 тыс. детей стали жертвами преступлений. Проблема обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

Почти 1,8 млрд. людей в мире подключены к интернету. Ежегодно растет число пользователей, среди которых все больше - детей и подростков. В России восемьдесят пять процентов российских детей в возрасте от 10 до 17 лет активно пользуются Интернетом. По статистическим данным в Сети они проводят до 25 часов в неделю и, как правило, пользуются Интернетом бесконтрольно.

В современных условиях развития общества компьютер стал для ребенка и «другом», и «помощником», и даже «воспитателем», «учителем». Всеобщая информатизация и доступный, высокоскоростной Интернет уравнял жителей больших городов и малых деревень в возможности получить качественное образование. Прилежные дети в 2 раза чаще попадают на «плохие» сайты в силу природной любознательности.

Более 20% детей становятся жертвами нападок со стороны сверстников.

80% школьников имеют аккаунты в социальных сетях.

70% в своих аккаунтах указывают свою фамилию, точный возраст и номер школы.

40% российских детей готовы продолжить онлайн общение в реальной жизни.

У 30% школьников данные аккаунта открыты всему миру. Более 28% опрошенных детей готовы переслать свои фотографии незнакомцам в Сети.

17% без колебаний соглашаются сообщить информацию о себе и своей семье - место жительства, профессия и график работы родителей, наличие в доме ценных вещей и т. д. (о том, для чего посторонним может потребоваться такая информация, дети, как правило, не задумываются).

22% детей периодически попадают на сайты для взрослых.

28% детей, увидев в интернете рекламу алкоголя или табака, хоть раз пробовали их купить, а 11% - пытались купить наркотики.

Около 14% опрошенных время от времени отправляют платные SMS за бонусы в онлайн-играх и лишь немногие обращают внимание на стоимость такой опции.

Классификация интернет-угроз

Во Всемирной паутине существует определённая классификация Интернет угроз. Юных пользователей сети могут подстерегать опасности. Их условно можно разделить на интернет-угрозы, связанные с безопасностью компьютера, с которого совершается выход в интернет, и интернет-угрозы психологического характера для детей и молодежи. Классификация угроз в Сети по четырем группам риска: контентные риски, коммуникационные риски, электронные риски, потребительские риски.

Некоторые Интернет-ресурсы могут причинить вред здоровью и развитию детей и подростков. Одни вовлекают детей в зависимость, другие разжигают национальную рознь, третьи негативно влияют на их психическое развитие, разрушают способность к реальному общению, влияют на мировоззрение, а также предлагают различные виды мошенничества и т. д.

Отказываться от благ информационных технологий бессмысленно, но бесконтрольный доступ детей к Интернету может привести к:

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

Как защитить детей от информации, причиняющей вред их здоровью и развитию, какие меры нужно принимать, чтобы уберечь их от пропаганды насилия и жестокости в журналах, газетах, Интернете и других средствах массовой информации?

В последние годы в мире и стране принят ряд важнейших законодательных актов, направленных на предупреждение наиболее серьезных угроз здоровья детей. Созданы новые государственные и общественные институты: учреждена должность Уполномоченного при Президенте Российской Федерации по правам ребенка, в ряде субъектов Российской Федерации создан институт уполномоченного по правам ребенка, учрежден Фонд поддержки детей, находящихся в трудной жизненной ситуации. Увеличился объем финансирования социальных расходов из федерального бюджета и бюджетов субъектов Российской Федерации, приняты новые меры социальной поддержки семей с детьми.

Согласно российскому законодательству информационная безопасность детей - это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию. Обеспечение государством информационной

безопасности детей, защита их физического, умственного и нравственного развития во всех аудиовизуальных медиа-услугах и электронных СМИ - это требование международного права (Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 «О защите несовершеннолетних и их человеческого достоинства в Интернете»),

Федеральный закон Российской Федерации от 28 июля 2012 г. N 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» охватывает практически все виды информационной продукции, включая СМИ, Интернет, сотовую связь и др. Он вносит изменения во многие законные акты Российской Федерации. Поправки, внесенные в закон «О защите детей от информации, причиняющей вред их здоровью и развитию» (29 декабря 2010 года № 436-ФЗ), впервые более подробно регламентируют способы маркировки контента и описывают процедуры экспертизы «информационной продукции».

Законом вносится предложение об ограничении в Сети «мест доступных для детей» и предусматривается ответственность операторов и администраторов Сайтов, которые не принимают административных и организационных мер, технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и развитию.

Обеспечение безопасности детей в СМИ и Интернет

Одним из основных направлений в борьбе за информационную безопасность детей является просвещение родителей. По данным статистики, половина российских подростков знает о Всемирной паутине и умеет работать в ней гораздо больше и лучше своих мам и пап. Уровень знаний родителей о программах и модулях по защите детей от негативной информации также очень и очень низкий. Сегодня многие из них встают перед проблемой: как же ограничить доступ ребенка к компьютеру, как ограничить время, пребывания в Интернет и защитить от порно-наркотиков-матов? Присмотр за детьми в интернете называется термином «родительский контроль».

Родительский контроль - это программы и службы, которые позволяют родителям и опекунам отслеживать, как ребенок использует компьютер: от фильтрации веб-содержимого и управления контактами электронной почты до ограничений на общение детей через Интернет.

Цель таких средств - обеспечить безопасность ребенка в Интернете**.** Эти инструменты иногда называют семейными настройками или настройками семейной безопасности. Существует множество программ по родительскому контролю, многие из них являются частью программ-антивирусов. Некоторые функции родительского контроля предусмотрены в операционной системе. Но настоящий родительский контроль обеспечивают только специализированные программы:

Анаферон http://netkidscontrol.ru/anaferon для блокировки сайтов, потенциально опасных для здоровья и психики учащихся.

Инетернет-фильтры (Интернет Цензор и NetPolice).

В основе работы программы Интернет Цензор лежит технология «бе-

лых списков», гарантирующая 100% защиту от опасных и нежелательных материалов. Программа содержит уникальные, вручную проверенные «белые списки», включающие все безопасные сайты Рунета и основные иностранные ресурсы. Программа надежно защищена от взлома и обхода фильтрации. Интернет Цензор может использоваться как в домашних условиях, так и в организациях - образовательных учреждениях, библиотеках, музеях, интернет-кафе и иных местах, где возможно предоставление несовершеннолетним доступа в Интернет.

NetPolice — программное обеспечение для фильтрации сайтов по их содержимому, не позволяет получить доступ к определённым сайтам или услугам сети Интернет. Система позволяет блокировать веб-сайты с содержимым, не предназначенным для просмотра. http://netpolice.ru — официальный сайт интернет-фильтра NetPolice.

В рамках проекта «Ребенок в Сети» каждый пользователь может бесплатно скачать и установить новое комплексное решение безопасности Panda Internet Security 2012, которое предоставляет максимальную защиту от всех типов угроз, включая защиту от вирусов, шпионов, хакеров, спама, мошенников и пр. Функция родительского контроля позволяет не только ограничить ребенка от доступа к нежелательным сайтам в Интернете (порнография, наркотики, онлайн-казино и пр.), но и дистанционно подключаться к компьютеру.

Возраст детей от 7 до 8 лет

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям (законным представителям) особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т. е. Родительским контролем.

При этом важно, чтобы у ребенка не было ощущения, что за ним ведется постоянное наблюдение. Однако, родителям полезно знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернет, используя электронную почту, заходить на сайты и чаты.

Рекомендации по безопасности детей от 7 до 8 лет

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
2. Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому что вам этого хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
3. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
4. Используйте специальные детские поисковые машины.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.

7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.

8. Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

9. Научите детей не загружать файлы, программы или музыку без вашего согласия.

10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.

11. В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

12. Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.

13. Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых»;

14. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст детей от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Рекомендации по безопасности детей от 9 до 12 лет

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

2. Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

3. Покажите ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Не забывайте беседовать с детьми об их друзьях в Интернет.

7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет.

8. Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.

9. Приучите детей никогда не выдавать личную информацию средст-

вами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.

10. Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

11. Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.

12. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

13. Расскажите детям об опасности порнографии в Интернет.

14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами;

15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Правила работы в сети Интернет

1. Не входите на незнакомые сайты.
2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.
3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.
4. Никогда не посылайте никому свой пароль.
5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.
6. При общении в Интернет не указывайте свои личные данные, а используйте псевдоним (ник).
7. Без контроля взрослых ни в коем случае не встречайтесь с людьми, с которыми познакомились в сети Интернет.
8. Если в сети необходимо пройти регистрацию, то постарайтесь выполнить ее так, чтобы в ней не было указано никакой личной информации.
9. Не всей информации, которая размещена в Интернете, можно верить.
10. Не оставляйте без присмотра компьютер с важными сведениям на экране.
11. Не сохраняйте важные сведения на общедоступном компьютере.

Рекомендации родителям

1. Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет.
2. Объясните детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством.
3. Объясните ребенку, что при общении в чатах, использовании про-

грамм мгновенного обмена сообщениями, использовании онлайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации.

4. 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.

5. Объясните своему ребенку, что в реальной жизни и в Интернет нет разницы между неправильными и правильными поступками.

6. Научите ваших детей уважать собеседников в Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни.

7. Скажите им, что никогда не стоит встречаться с друзьями из Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают.

8. 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.

9. 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.