Утверждаю:
Директор МБОУ С(К)ОШ г. Нытва
«27» августа 2018г
_____ О.С. Курпульская

План работы по информационной безопасности МБОУ С(К)ОШ г. Нытва на 2018-2019 уч. год

№ п/п	Наименование мероприятий	сроки	ответственный
Организационные мероприятия			
1	Организаия инструктажа педагогов по медиабезопасности в том числе по использованию лицензионного програмного обеспечения и соблюдению ФЗ № 52	сентябрь	администрация
2	Организация защиты персональных данных сотрудников, обучающихся и их родителей при их обработке в информационных системах.	В течение учебного года	Классные Руководители, заместители директора, секретарь-делопроизводитель
3	Обеспечение контроля безопасности содержания приобретаемой информационной продукции для детей в соответствии с возрастными категориями	Постоянно	Заместители директора
4	Организация и обеспечение контроля за соответствием содержания сайта школы требованиям законодательства	В течение учебного года года	Ответственный за сайт
Работа с родителями			
5	Тематические родительские собрания, посвященных защите детей от негативного контента в СМИ	Ежегодно	Заместители директора, классные руководители
6	Тематические консультации для родителей «Поведенческие и психологические индикаторы признаков насилия и жестокого обращения с детьми»	В течение учебного года	Педагог-психолог
7	Беседы с родителями по безопасному использованию сети «Интернет»	Один раз в четверть	Классные руководители
8	Распространение тематических буклетов о правах детей, по пропаганде ответственного родительства, профилактике семейного насилия, жестокого обращения с детьми и др.	Один раз в четверть	Классные руководители
9	Проведение лектория для! родителей учащихся по режиму доступа детей к образовательным ресурсам	Сентябрь	Социальный педагог
Работа с обучающимися			

10	Правовой час «Права свои знай, обязанности не забывай»	Сентябрь	Классные руководители
11	Всероссийский урок безопасности школьников в сети Интернет	30.10	Соц. педагог, классные руководители
12	Изготовление и распространение буклетов с информацией о безопасном интернете для детей	Март	Социальный педагог
13	Классные часы: «Киберугрозы современности: главные правила их распознавания и предотвращения»	3 четверть	Социальный педагог
14	Проведение инструктажей по доступу к образовательным ресурсам Интернет	В течение учебного года года	Классные руководители

Классификация Интернет-угроз

Контентные риски 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.

Электронная безопасность Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в сеть домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн-мошенничество и спам.

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.

Спам Спам - это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, 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. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг.

Коммуникационные риски Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя контакты педофилов с детьми и киберпреследования.

Незаконный контакт 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.

Памятка по безопасному поведению в Интернете

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, вы должен предпринимать следующие меры предосторожности при работе в Интернете:

1. Когда ты регистрируешься на сайтах, старайся не указывать персональную информацию в Интернете. Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.
2. Используй веб - камеру только при общении с друзьями. Проследи, чтобы посторонние люди не имели возможности видеть ваш разговор, так как он может быть записан.
3. Ты должен знать, что если ты публикуешь фото или видео в Интернете - каждый может посмотреть их.
4. Нежелательные письма от незнакомых людей называются «Спам». Если ты получил такое письмо, не отвечай на него. Если ты ответишь на подобное письмо, отправитель будет знать, что ты пользуешься своим электронным почтовым ящиком, и будет продолжать посылать тебе спам.
5. Если тебе пришло сообщение с незнакомого адреса, его лучше не открывать. Вы не можете знать, что на самом деле содержат эти файлы. В них могут быть вирусы или фото/видео с «агрессивным» содержанием.
6. Не добавляй незнакомых людей в свой контакт.
7. Если тебе приходят письма с неприятным и оскорбляющим тебя содержанием, если кто-то ведет себя в твоем отношении неподобающим образом, сообщи об этом взрослым.
8. Если рядом с тобой нет взрослых, не встречайся в реальной жизни с людьми, с которыми ты познакомился в Интернете. Если твой виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к твоей заботе о собственной безопасности!
9. Никогда не поздно рассказать взрослым, если тебя кто-то обидел или расстроил.

Памятка для обучающихся начальной школы

1. Всегда помни своё Интернет - королевское имя (e-mail, логин, пароли) и не кланяйся всем подряд (не регистрируйся везде без надобности)!
2. Не поддавайся ярким рекламам - указателям и не ходи тропками, путанными на подозрительные сайты: утопнуть в трясине можно!
3. Если пришло письмо о крупном выигрыше – это «Лохотрон - грамота»: просто так выиграть невозможно, а если хочешь зарабатывать пиастры, нужно участвовать в полезных обучающих проектах!
4. Чтобы не забыть тропинку назад и вернуться вовремя, бери с собой Клубок волшебный (заводи себе будильник, садясь за компьютер)!
5. Если хочешь дружить с другими царствами-государствами, изучай полезные социальные сервисы Web 2.0: они помогут тебе построить «Мой королевский мир», свой царский блог, форум для глашатаев важных – друзей званных!
6. Не забывай обновлять антивирусную программу – иначе вирус Серый Волк съест весь твой компьютер!
7. Не скачивай нелицензионные программные продукты – иначе пираты потопят твой корабль в бурных волнах Интернет!

Памятка для родителей

В памятке представлены практические рекомендации о том, как помочь юным пользователям оставаться в безопасности в киберпространстве и избежать существующих рисков. Что делать, если ребенок все же столкнулся с какими-либо рисками?

Как защитить ребенка от нежелательного контента в Интернете

Контентные риски – это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику; информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

Как помочь ребенку избежать столкновения с нежелательным контентом:

Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации подобного рода. Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Приучите их спрашивать о том, в чем они не уверены. Старайтесь спрашивать ребенка об увиденном в Интернете. Зачастую, открыв один сайт, ребенок захочет познакомиться и с другими подобными ресурсами. Включите программы родительского контроля и безопасного поиска, которые помогут оградить ребенка от нежелательного контента.

Постоянно объясняйте ребенку правила безопасности в Сети. Помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую может быть гораздо конструктивнее, чем постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.

Используйте специальные настройки безопасности (инструменты родительского контроля, настройки безопасного поиска и др.).

Выработайте «семейные правила» использования Интернета. Ориентируясь на них, ребенок будет знать, как поступать при столкновении с негативным контентом.

Будьте в курсе того, что ваш ребенок делает в Интернете. Чаще беседуйте с ребенком о том, что он делает в Сети.

Как научить ребенка быть осторожным при знакомстве с новыми людьми в Интернете

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др.

Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы. Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство, чаще всего, происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Предупреждение груминга:

Будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются;

Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать интернет-знакомым свои фотографии;

Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу. Не позволяйте вашему ребенку встречаться с онлайн-знакомыми без вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу. Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Объясните ребенку основные правила поведения в Сети:

- ✓ ***нельзя делиться с виртуальными знакомыми персональной информацией, а встречаться с ними в реальной жизни следует только под наблюдением родителей;***
- ✓ ***если интернет-общение становится негативным – такое общение следует прервать и не возобновлять.***

Как избежать кибербуллинга

Кибербуллинг – преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Предупреждение кибербуллинга:

- объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости так же неприятно, как и слышать;

- научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Возможно, стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем;
- если ребенок стал жертвой буллинга, помогите ему найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички.
- объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз;
- старайтесь следить за тем, что ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

Как защититься от кибербуллинга:

Не провоцировать. Общаться в Интернете следует этично и корректно. Если кто-то начинает оскорблять ребенка в Интернете – необходимо порекомендовать уйти с такого ресурса и поискать более удобную площадку.

Если по электронной почте или другим каналам кто-то направляет ребенку угрозы и оскорбления – лучше всего сменить электронные контакты (завести новый e-mail, Skype, ICQ, новый номер мобильного телефона).

Если кто-то выложил в Интернете сцену киберунижения ребенка, необходимо сообщить об этом администрации ресурса. Можно также обратиться на горячую линию. Даже при самых доверительных отношениях в семье, родители иногда не могут вовремя заметить грозящую ребенку опасность, и тем более не всегда знают, как ее предотвратить.

Вот на что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:

- Беспокойное поведение. Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.
- Неприязнь к Интернету. Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.
- Нервозность при получении новых сообщений. Негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников

Кибермошенничество – один из видов киберпреступления, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и другое).

Предупреждение кибермошенничества:

* Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете.
* Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.
* Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности:

Ознакомьтесь с отзывами покупателей.

Проверьте реквизиты и название юридического лица – владельца магазина.

Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs).
Поинтересуйтесь, выдает ли магазин кассовый чек.
Сравните цены в разных интернет-магазинах.
Позвоните в справочную магазина.
Обратите внимание на правила интернет-магазина.
Выясните, сколько точно вам придется заплатить.
Объясните ребенку, что нельзя отправлять слишком много информации о себе при совершении интернет - покупок: данные счетов, пароли, домашние адреса и номера телефонов. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.

Как распознать интернет - и игровую зависимость

Сегодня в России все более актуальны проблемы так называемой «интернет – зависимости» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет, и несущие убытки, в случае если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Как выявить признаки интернет - зависимости у ребенка:

- ✓ Оцените, сколько времени ребенок проводит в Сети, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.
- ✓ Поговорите с ребенком о том, чем он занимается в Интернете. Социальные сети создают иллюзию полной занятости – чем больше ребенок общается, тем больше у него друзей, тем больший объем информации ему нужно охватить – ответить на все сообщения, проследить за всеми событиями, показать себя. Выясните, поддерживается ли интерес вашего ребенка **реальными увлечениями**, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать, насколько важно для ребенка общение в Сети и не заменяет ли оно **реальное общение с друзьями**.
- ✓ Понаблюдайте за сменой настроения и поведением вашего ребенка после выхода из Интернета. Возможно проявление таких психических симптомов как подавленность, раздражительность, беспокойство, нежелание общаться. Из числа физических симптомов можно выделить головные боли, боли в спине, расстройства сна, снижение физической активности, потеря аппетита и другие.

Если вы обнаружили возможные симптомы интернет-зависимости у своего ребенка, необходимо придерживаться следующего алгоритма действий:
Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и так далее.
Не запрещайте ребенку пользоваться Интернетом, но постарайтесь установить **регламент пользования** (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения домашних уроков и прочее). Для этого можно использовать специальные программы родительского контроля, ограничивающие время в Сети.
Ограничьте возможность доступа к Интернету только своим компьютером или компьютером, находящимся в общей комнате, – это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает ребенок.
Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в Интернете. Это поможет наглядно увидеть и осознать проблему, а также избавиться от некоторых навязчивых действий, например от бездумного обновления странички в ожидании новых сообщений.
Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. ***Попробуйте перенести кибердеятельность в реальную жизнь.*** Например, для многих компьютерных игр существуют аналогичные настольные игры, в которые можно играть всей

семьей или с друзьями, при этом общаясь друг с другом вживую. Важно, чтобы у ребенка были не связанные с Интернетом увлечения, которым он мог бы посвящать свое свободное время.
Дети с интернет - зависимостью субъективно ощущают невозможность обходиться без Сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без Интернета. Важно, чтобы ребенок понял – ничего не произойдет, если он на некоторое время выпадет из жизни интернет - сообщества.

В случае серьезных проблем обратитесь за помощью к специалисту.

Как научить ребенка не загружать на компьютер вредоносные программы

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными, и даже использовать ваш компьютер для распространения вируса, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.
Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.
Периодически старайтесь полностью проверять свои домашние компьютеры.
Делайте резервную копию важных данных.
Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

Что делать, если ребенок все же столкнулся с какими-либо рисками.

Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и знать, что вы хотите разобраться в ситуации и помочь ему, а не наказать.
Постарайтесь внимательно выслушать рассказ о том, что произошло, понять, насколько серьезно произошедшее, и насколько серьезно это могло повлиять на ребенка.
Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или попал в неприятную ситуацию (потратил ваши или свои деньги в результате интернет - мошенничества и прочее) – постарайтесь его успокоить, и вместе с ним разберитесь в ситуации: что привело к данному результату, какие неверные действия совершил сам ребенок, а где вы не рассказали ему о правилах безопасности в Интернете.
Если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и тому подобное), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время.
Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств: зайдите на страницы сайта, где был ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться (например, для обращения в правоохранительные органы);
Если вы не уверены в оценке серьезности произошедшего с вашим ребенком, или ребенок недостаточно откровенен с вами, или вообще не готов идти на контакт, или вы не знаете как поступить в той или иной ситуации – обратитесь к специалисту (телефон доверия, горячая линия и другое), где вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций (МВД, МЧС, Сестры и другие)

ЛИНИЯ ПОМОЩИ "ДЕТИ ОНЛАЙН"

1 февраля 2010 года в рамках Года Безопасного Интернета в России запущен всероссийский общественный проект- Линия помощи "Дети онлайн".

Телефон Линии помощи: 8-800-25-000-15.

Если вы нуждаетесь в консультации специалиста по вопросам безопасного использования Интернета, если ваш ребенок уже столкнулся с рисками в Сети, обратитесь на Линию помощи "Дети Онлайн" по телефону: **8 800 25 000 15 (звонок по России бесплатный).** Официальный сайт Линии помощи "Дети онлайн": www.detionline.org.