МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ЦЕНТР РАЗВИТИЯ ОБРАЗОВАНИЯ»
ГОРОД УСТЬ-ИЛИМСК

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Круглого стола

«С кого начинается информационная безопасность»

Усть-Илимск, 2023

Методические материалы заседания круглого стола «С кого начинается информационная безопасность» городского методического объединения классных руководителей

Предназначено для педагогических работников муниципальных общеобразовательных учреждений.

В соответствии с Приказом Управления образования Администрации города Усть-Илимск от 16.02.2023г. №172 «О проведении городского образовательного форума: «Единое образовательное пространство города (обучение и воспитание: стратегия и практика развития» в соответствии с планом работы Управления образования Администрации города Усть-Илимска на 2022-2023 учебный год, утвержденный приказом от 31.08.2022г. №619, руководствуясь Уставом Муниципального казенного учреждения «Центр развития образования»

Принято решение опубликовать на официальном сайте Управления образования
Администрации города Усть-Илимска http://uiedu.ru

Материалы печатаются в авторской редакции. За достоверность сведений, изложенных в материалах, несут ответственность авторы.

«Современные подходы к решению проблемы информационной безопасности школьника»

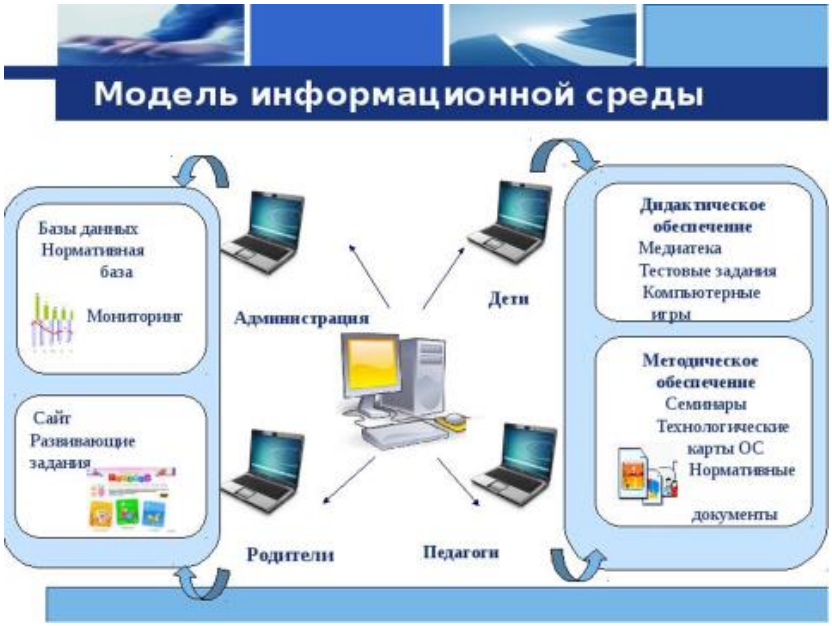
Чабан Людмила Алексеевна,

руководитель ГМО классных руководителей,

МАОУ СОШ № 11, учитель биологии и химии.

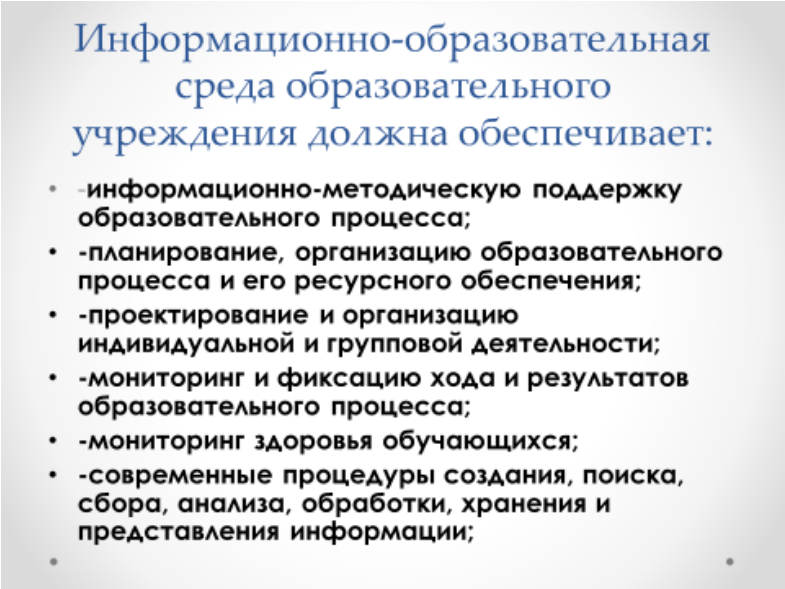
Становление информационного общества охватывает все сферы деятельности человека, в том числе и сферу образования, и основано на массовом внедрении компьютерной техники и использовании сети Интернет в образовательных учреждениях. Современная система школьного образования не может остаться в стороне от глобального процесса информатизации общества и образования, в качестве одной из сторон которого выступает расширение информационного образовательного пространства учебного заведения

В настоящее время жизнь развивается с такой скоростью, что за ней практически невозможно угнаться, и уже сейчас никто не может отрицать значение сети Интернет как всемирной информационной среды. Но, несмотря на глобальное значение Интернета у современного общества стали возникать проблемы с использованием сети.



В каждом образовательном учреждении создана и успешно функционирует информационно-образовательная среда. Ее значение в последнее время возрастает, она качественно влияет на образовательный процесс, всех субъектов образования и на их отношения в образовательной системе.

В соответствии с требованиями федерального государственного образовательного стандарта среднего (полного) общего образования информационно-образовательная среда образовательного учреждения включает: комплекс информационных образовательных ресурсов, в том числе цифровые образовательные ресурсы; совокупность технологических средств информационных и коммуникационных технологий: компьютеры, иное информационное оборудование, коммуникационные каналы; систему современных педагогических технологий, обеспечивающих обучение в современной информационно-образовательной среде.



Информационно-образовательная среда образовательного учреждения должна обеспечивает

-информационно-методическую поддержку образовательного процесса;

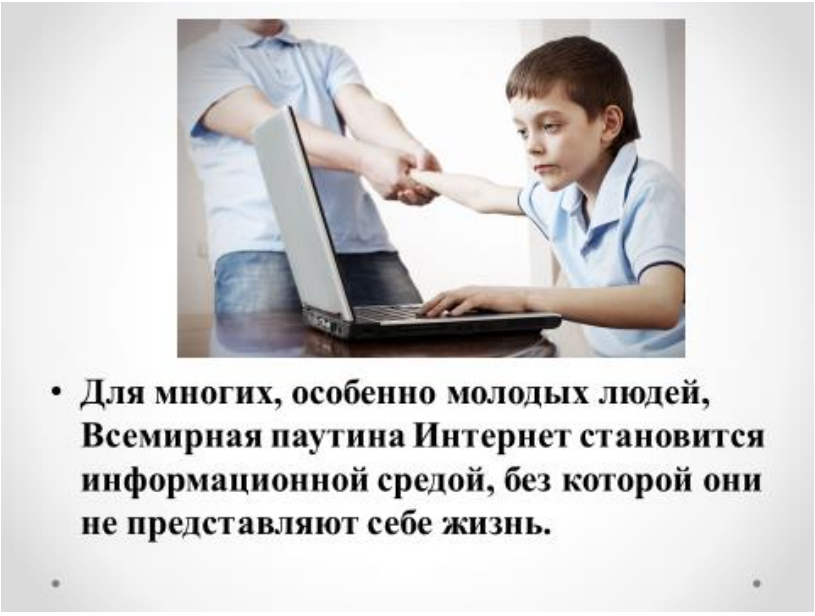
-планирование, организацию образовательного процесса и его ресурсного обеспечения

-проектирование и организацию индивидуальной и групповой деятельности;

-мониторинг и фиксацию хода и результатов образовательного процесса;

-мониторинг здоровья обучающихся;

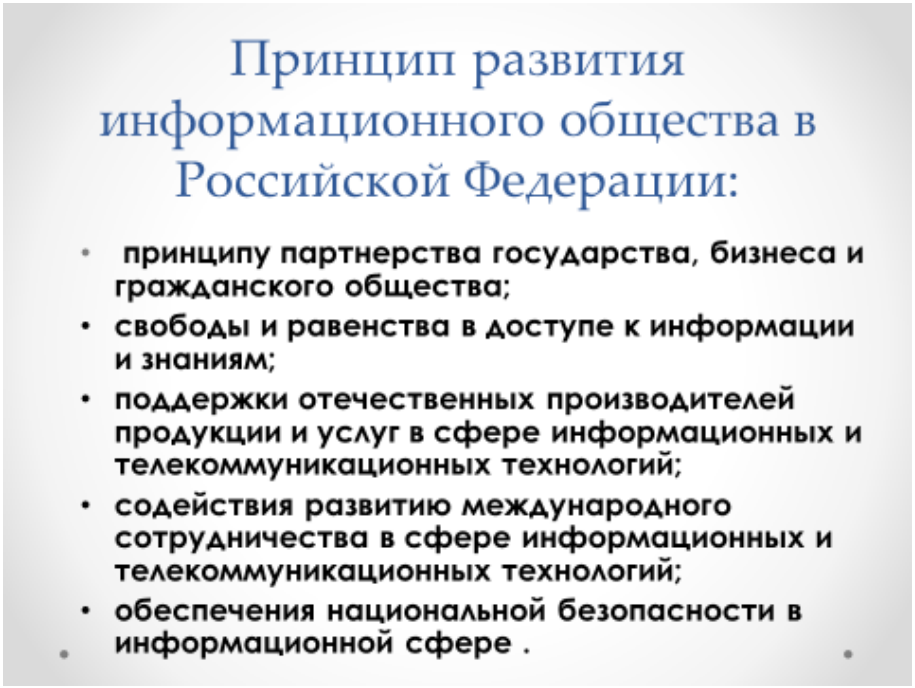
-современные процедуры создания, поиска, сбора, анализа, обработки, хранения и представления информации и т д



Личность ребенка, включенная в процесс познания, оказывается незащищенной от потоков информации, в связи с чем возникает острая необходимость расширения содержания общего среднего образования, введения в него новых компонентов, связанных с обучением информационной безопасности.

В тоже время количество угроз информационной безопасности растет сегодня с каждым днем по мере расширения информационной среды школы, активно протекающих процессов информатизации и глобализации.

С развитием информационно-коммуникативных технологий в системе образования все больше используется опыт, накопленный сетевыми сообществами в обучении и приобщении учителей и школьников к участию в жизни таких сообществ, существующих на базе сетевых центров науки, искусства, здравоохранения, профессионального образования, бюджетной сферы и бизнеса.



Развитие сетевых сообществ в образовательной среде будет способствовать формированию новых и развитию имеющихся профессиональных сообществ прежде всего за счет овладения в учебном процессе методологией, культурой, безопасностью работы в сетевых сообществах, что в общей сложности отвечает принципам развития информационного общества в Российской Федерации:

· принципу партнерства государства, бизнеса и гражданского общества;

· свободы и равенства в доступе к информации и знаниям;

· поддержки отечественных производителей продукции и услуг в сфере информационных и телекоммуникационных технологий;

· содействия развитию международного сотрудничества в сфере информационных и телекоммуникационных технологий;

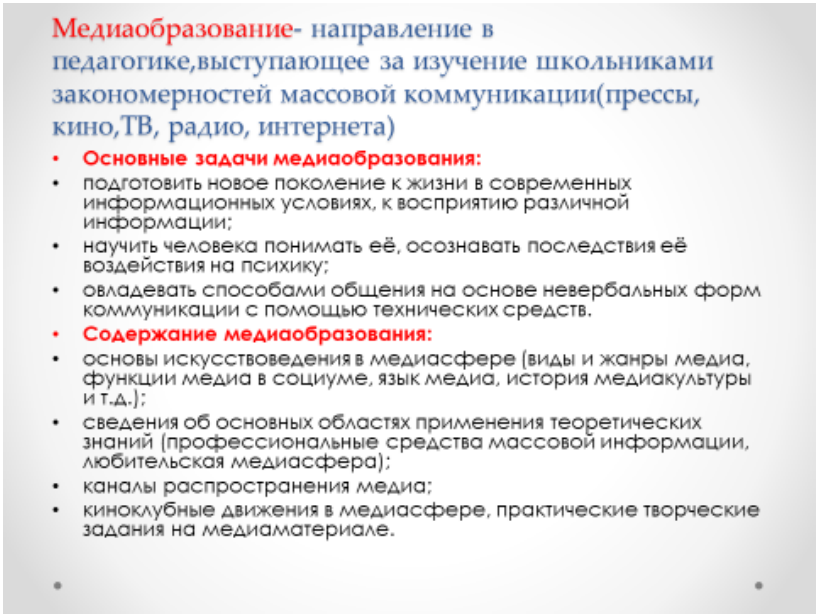
· обеспечения национальной безопасности в информационной сфере.

Профессиональная деятельность учителей в сети Интернет -- это прежде всего деятельность, направленная на учащихся, на развитие интереса к предмету, на развитие их мышления, творчества, коллективизма. Учитель организует своих учеников для участия в дистанционных олимпиадах, викторинах, конкурсах, направляет деятельность учащихся в телекоммуникационных проектах и формирует культуру общения в сетевых сообществах. Профессиональная деятельность учителей в сети Интернет включает деятельность, направленную на самих учителей, на самообразование, деятельность, связанная с повышением квалификации. Использование школьниками сети Интернет для получения новых знаний и установления лично значимых социальных контактов, направленных на повышение их уровня готовности к профессиональному самоопределению, способствует развитию информационной культуры подростков и положительно влияет на их ценностные ориентиры. Для обеспечения организационно-педагогической и информационной поддержки профессионального самоопределения старших школьников могут использоваться социальные сети и возможности технологий Web 2.0. Участвуя в блогах, организованных в социальных сетях, школьники имеют реальную возможность общения в интерактивном режиме с представителями различных профессиональных сообществ. От них подростки могут получать информацию

о личных и профессиональных качествах, необходимых специалистам данной сферы деятельности, о путях получения той или иной профессии.

Глобальная сеть наряду с уникальными возможностями, которые с ее помощью открываются для системы образования, таит в себе и чрезвычайную опасность. Опасность эта кроется не в самом компьютере (например, свойствах излучения: они не больше, чем у телевизора), а именно в информации, которая размещается в сетях, доступ к которой открыт для всех желающих. Все больше школьников пользуются информацией Всемирной паутины, которая сказывается на интеллектуальном, нравственном развитии детей, их психическом и физическом здоровье. Разработчики порталов, предоставляющие информационные сервисы для детей, озабочены вопросами информационной безопасности своих пользователей. Особенности восприятия информации в детском возрасте, когда значительное место занимает непосредственный интерес к теме, ее эмоциональная окраска, доминирование иррационального мышления во многих случаях не позволяют детям отнестись серьезно к рекомендуемым правилам обеспечения информационной безопасности и самостоятельно оценить их важность.

Последовательному формированию у школьников самостоятельного критического мышления может способствовать введение в школьные программы курса медиаобразования. Медиаобразование -- это предметная область, изучающая специфику языка различных средств массовой информации, в первую очередь телевидения, радио, прессы, Интернета. Базовым умениям работы с информацией необходимо обучать учащихся, начиная с начальной школы (уметь выделять главную мысль в тексте, сделать вывод, дать оценку событию и т.д.). Это должна быть системная работа. Вся система обучения должна быть настроена на формирование этих базовых умений. Мировая педагогическая общественность давно осознала значимость этой проблемы не только для интеллектуального развития человека, но и для его информационной безопасности. Так, проблема информационной безопасности ребенка перерастает в проблему концепции системы образования, системы подготовки педагогических кадров.

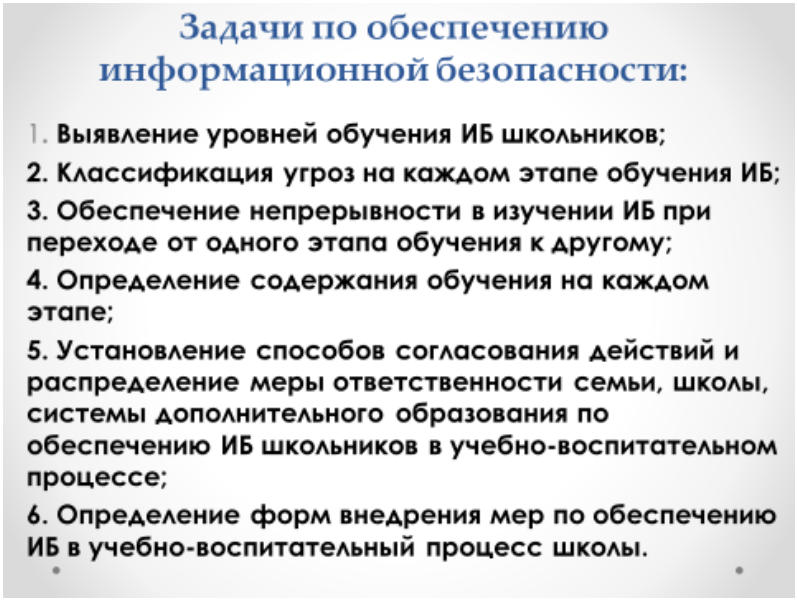


В процессе непрерывного образования личность должна получить знания, выработать умения и навыки работы с новыми информационными технологиями и средствами телекоммуникации, позволяющими выполнять социальные роли создателя и потребителя информации. Данный процесс не ограничивается только реализацией технологических проблем, он включает в себя овладение эффективными методами обучения и познания, деятельности и мышления, стоящими на верхушке пирамиды непрерывного образования, а именно: анализа, синтеза, абстрагирования, формализации, обобщения информации, связанных с креативным уровнем образования, позволяющим из множества информации строить свое представление о мире или, иначе, сформировать информационный стиль мышления и информационное мировоззрение .

В информационной сфере наблюдаются многие негативные явления, для преодоления их последствий необходимо выработать механизмы защиты психики личности, сознания, духовной жизни от информационных манипуляций и агрессии массовой культуры, воздействия недостоверной, ложной информации, дезинформации. Информационная безопасность предполагает также защиту личности от неправомерного вмешательства в производство информации и неправомерного доступа к персональным

информационным ресурсам, замены реальной жизни виртуальной (иллюзорной). Результатом непрерывного образования является формирование у личности когнитивных структур, представляющих собой относительно стабильные психологические системы репрезентации знаний, которые вместе с тем являются системами извлечения и анализа информации.

С момента поступления ребенка в школу угроза информационной безопасности в отношении ребенка возрастает, поскольку у него появляется свобода от наблюдения и контроля со стороны родителей, а также начинает разграничиваться сфера влияния семьи, школы, системы дополнительного образования, социума. Вследствие неразработанности проблемы обеспечения непрерывной информационной безопасности школьников и методики ее комплексной реализации на уровне семьи и школы ответственность за ребенка педагоги нередко перекладывают на родителей, а родители -- на педагогов и работников системы дополнительного образования.



Таким образом, выделим следующие задачи по обеспечению информационной безопасности школьников в непрерывном общем образовании и наметим возможные пути решения поставленных задач обеспечения ИБ школьников.

1. Выявление уровней обучения ИБ школьников. В школе можно выделить три уровня обучения ИБ, соответствующие: 1) начальной школе, 2) неполной средней школе, 3) средней общеобразовательной и профессиональной школе.

2. Классификация угроз на каждом этапе обучения ИБ. На первом этапе можно выделить угрозы личной безопасности школьника, не связанные с использованием технических средств. На втором этапе выделяют угрозы личности, семье, окружающему ученика социуму, возникающие при работе с информацией на компьютере и в Интернете. На третьем этапе -- изучение основ профессиональной безопасности по выбранному профилю с использованием специальных средств записи и обработки информации. Второй и третий этапы обучения информационной безопасности непосредственно связаны с медиаобразованием.

3. Обеспечение непрерывности в изучении ИБ при переходе от одного этапа обучения к другому. Обеспечение непрерывного обучения за счет четкого выделения понятийного аппарата на каждом этапе и построении на его основе

системы последующих положений с учетом возрастных особенностей развития и использования технических средств работы с информацией. Определение роли угроз исходящих от сообществ, в которые могут входить школьники на каждом этапе непрерывного образования.

4. Определение содержания обучения на каждом этапе. В зависимости от возникающих угроз ИБ (вторая задача) необходимо определить содержание обучения ИБ на каждом этапе и разработать условия безопасного использования соответствующих сервисов работы с образовательным контентом. Особенностью обучения ИБ является то, что недостаточно изучить только организационные и технические средства обеспечения ИБ, но и необходимо привить нравственность и воспитать ответственность за использование информации, которая может причинить ущерб не только личности, неумело с ней обращающейся, но и другим людям.

5. Установление способов согласования действий и распределение меры ответственности семьи, школы, системы дополнительного образования по обеспечению ИБ школьников в учебно-воспитательном процессе. Необходимо разработать методические рекомендации для родителей по обеспечению информационной безопасности семьи. Они должны содержать классификацию возможных информационных угроз. Рекомендации по ограничению доступа ребенка к информации и по обеспечению информационной безопасности для детей, находящихся за пределами школы, -- в зоне ответственности родителей. Организационными формами взаимодействия школы с родителями по вопросам обеспечения ИБ как учащихся, так и семьи в целом могут быть как традиционные (родительские собрания, заседания родительских комитетов, индивидуальные беседы учителей с родителями), так и специально организованные лекции и семинары с участием педагогов, правоохранительных органов, специалистов по защите информации.

6. Определение форм внедрения мер по обеспечению ИБ в учебно-воспитательный процесс школы. Необходимо разработать систему дидактических средств для учащихся по обеспечению ИБ на каждом этапе обучения, включающую в себя систему понятий, способы поведения, законодательство в области ИБ, и другие аспекты. Внедрение знаний по ИБ в учебный процесс школы может быть как в рамках существующих предметов, например информатики или ОБЖ, так и на специально организуемых занятиях, например, классных часах, ролевых играх, проектной деятельности учащихся.

Комплексное решение рассмотренных задач информационной безопасности со стороны семьи и школы позволит значительно уменьшить риски причинения различного рода ущербов (морального, материального, здоровью и др.) ребенку. Поэтому обеспечение информационной безопасности школьников должно стать одним из первоочередных направлений работы современной школы.

- **Люби жизнь!**
- **Общайся с живой природой!**
- **Твори!**

«Формирование информационного иммунитета: проблемы и пути их решения»

Голос Г.И., руководитель ГМО учителей информатики, руководитель творческой группы проекта Сетевого взаимодействия ГПС, МБОУ «СОШ № 8 имени Бусыгина М.И.»

Стремительное развитие компьютерных технологий, наряду с глобальной информатизацией общества, качественно меняет окружающую нас жизнь и порождает множество новых проблем, в частности, проблему формирования информационной культуры и безопасности среди подрастающего поколения.

На данный момент в мире возникло устойчивое понимание того, что проблема безопасности детей в интернете — это проблема, требующая срочного вмешательства специалистов. Самым эффективным механизмом решения этой проблемы может и должно стать формирование информационной культуры личности — родителей и детей, а также профессиональной информационной культуры учителей.

Обратимся к официальной статистике.

Опрос ВЦИОМ[1] показал, что две трети подростков 14-17 лет (67%) ежедневно проводят в интернете более 4 часов. Среди людей старше 18 лет таковых гораздо *меньше – 30%.*

Те, кто выходит в интернет, часто пользуются соцсетями. В них ежедневно бывают 89% подростков 14-17 лет и 53% тех, кто старше 18 лет.

Только 1% пользующихся интернетом подростков не выходят в соцсети, еще 1% выходят редко (но чаще чем раз в месяц) и 9 % выходят несколько раз в неделю.

[1] По данным на 2022 год, декабрь.

Среди пользующихся интернетом старше 18 лет отношения с соцсетями такие: 20% не пользуются, 4% - выходят в них раз в месяц и реже, 7% - несколько раз в месяц и 15% - несколько раз в неделю.

Являясь классным руководителем 5 «а» класса, мною была проведена *диагностика* как учеников, так и их родителей на предмет пользования сетью Интернет: *содержание контента, частота посещения, меры предосторожности, правила пользования информацией в сети* (Приложение 1).

Проанализировав результаты, можно сделать следующие *выводы:*

– около трети (37%) подростков 11-13 лет ежедневно подолгу «зависают» в Интернете и пользуются соцсетями, онлайн играми, причем большая их часть контролируется родителями;

– больше половины опрошенных (62%) знают, как уберечь личную информацию от мошенников и правила поведения в сети.

В свою очередь, *родители* обеспокоены *следующим*:

– около 40% считают, что долгое времяпрепровождение в сети отрицательно сказывается на здоровье детей как физическом, так и психоэмоциональном;

– большинство (81%) уверены, что Интернет оказывает влияние на формирование мировоззрения у детей.

– наибольшую опасность представляют сайты, которые имеют: (*по убыванию*): доступ к нежелательному содержимому (порнография, азартные игры, наркотики, насилие, националистическая или фашистская идеология); сообщение конфиденциальной информации собеседникам в сети (полное имя, адрес, номер интернет-кошелька, банковской карты родителей, места прогулок, время возвращения домой членов семьи) и контакты с незнакомыми людьми посредством чатов, электронной почты и т.д. (среди них могут быть как мошенники, выпытывающие конфиденциальную информацию, так и люди с психическими расстройствами), менее всего - угроза заражения компьютера вредоносным ПО (программным обеспечением).

Стоит отметить, что согласно опросу (*Приложение 1*) главную роль в формировании информационной культуры и информационной грамотности родители отводят *учителям (классным руководителям)*: проведение тематических классных часов; организация/активное использование учителем информационных ресурсов, отвечающих образовательным потребностям современного школьника; разбор сложных ситуаций, при которых возможна потеря данных и заражение компьютера; положительный пример общения в сетевом пространстве.

В связи с этим выделены несколько *задач:*

– формирование *целостного* представления о правилах поведения в сети интернет (ознакомить учащихся и их родителей с Федеральным законом Российской Федерации № 436-ФЗ от 29 декабря 2010 года «О защите детей от информации, причиняющей вред их здоровью и развитию» и Федеральным законом Российской Федерации от 21 июля 2011 г. № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»);

– развитие медиакомпетентности;

– формирование целостного представления о способах защиты персональных данных.

Решение данных задач осуществляется на нескольких *уровнях.*

Всероссийский уровень

Олимпиада «Безопасный интернет» для учеников 1-9 классов на платформе Учи.ру (https://uchi.ru/).

Международный Квест по цифровой грамотности «Сетевичок» https://сетевичок.рф.

Контрольная работа по теме «Информационная безопасность» https://единыйурок.дети/component/k2/item/17-edinyj-urok-po-bezopasnosti-v-seti-internet.

Региональный уровень

Квест по информационной безопасности https://quest.belov.site/

Муниципальный уровень

Викторина-поиск «Безопасность в сети Интернет».

Классные часы:

«Медиаграмотность и цифровая гигиена» в рамках занятий «Разговоры о важном» https://razgovor.edsoo.ru/topic/34/.

Участие в сетевом проекте «Безопасность в сети Интернет», авторская разработка https://sites.google.com/site/school14lesson/home.

Важной частью по формированию *информационного иммунитета* является разработка памяток (Приложение 2).

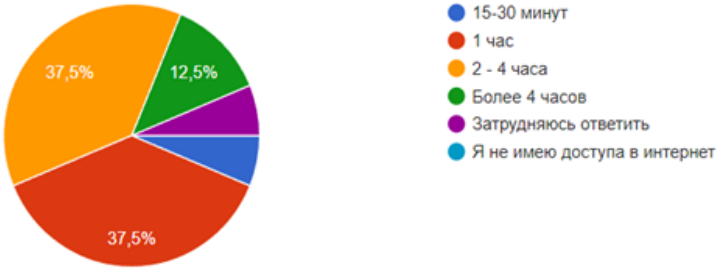
В заключение хочется сказать, что сегодня Интернет – один из главных инструментов для общения и поиска информации. Защита детей в сети Интернет – это проблема, с которой сейчас сталкиваемся все мы.

Грамотное использование современных технологий при работе с информацией через урочную и внеурочную деятельность, *систематическая совместная* (родитель-ребенок-классный руководитель/учитель) *деятельность*, направленная на *овладение* информационной культуры как информационного мировоззрения, предполагающего обязательную мотивацию личности на необходимость специальной информационной подготовки, безусловно, способствуют формированию информационного иммунитета подростка.

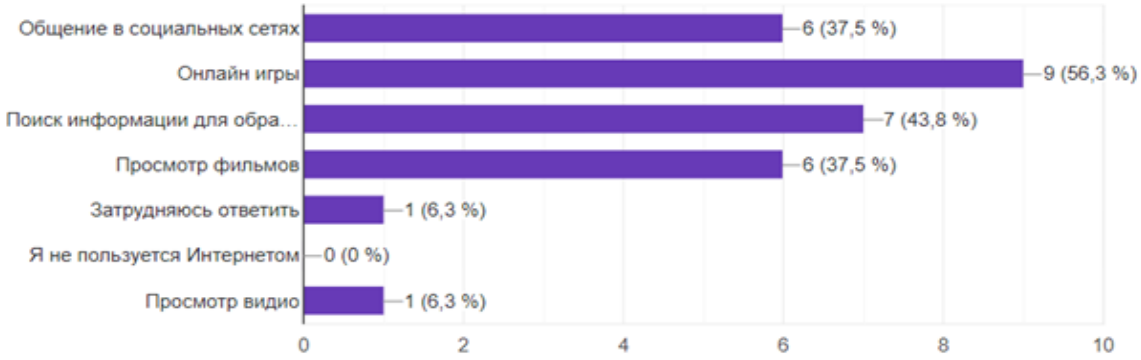
Приложение 1.

Опрос учащихся (часть ответов)

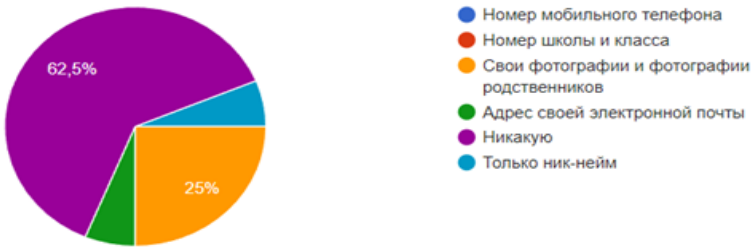
Сколько (преимущественно) времени в день Вы проводите в Интернете?



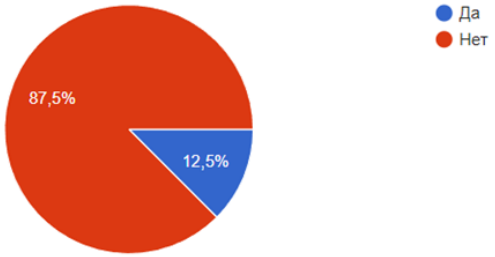
На какой вид деятельности в интернете Вы тратите наибольшее количество времени? Вы можете выбрать несколько вариантов



Какую информацию Вы размещаете в открытом доступе?

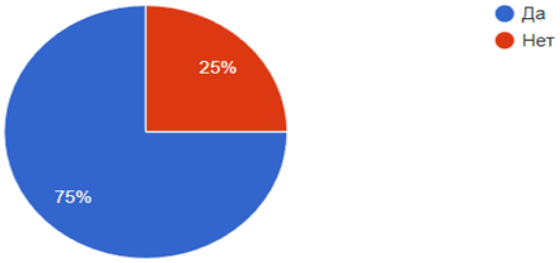


Совершали ли Вы покупки в интернет магазинах самостоятельно?

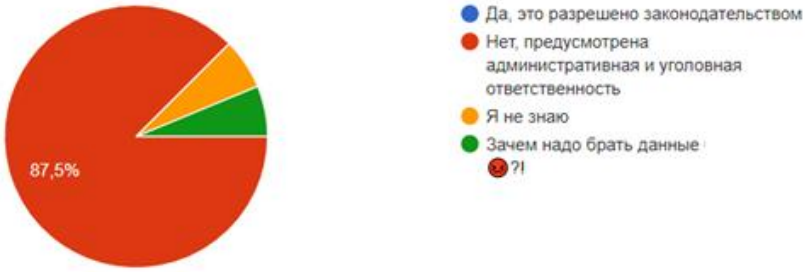


В каком виде Вы храните свои пароли?

Знаете ли вы как защитить себя от интернет-мошенников?



Можно ли без разрешения размещать фото одноклассников в сети, использовать чужую информацию в своих целях?



Знаете ли вы правила поведения в сети?
Если да, то какие (перечислите в строчку)

Придерживайтесь в сети тех же правил поведения, которым вы следуете в реальной жизни ...
Думайте о своих собеседниках ...
Покажите себя с лучшей стороны ...
Сначала читайте, затем спрашивайте ...
Не забывайте об орфографии и пунктуации ...
Уважайте личные данные других.

Не сохранять и не открывать подозрительные файлы, никому не сообщать свой пароль, не заходить на подозрительные сайты и не сообщать свои персональные данные.

Не оскарблять

Не писать гадости

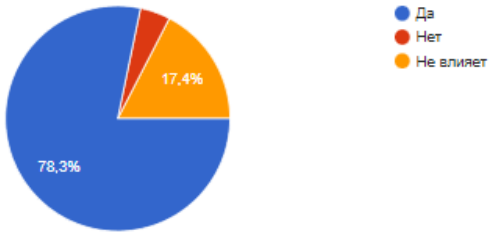
Не посещать ненужные сайты

Не разговаривать с незнакомыми, не давать свою личную информацию, соблюдать нормы речи.

Опрос родителей (часть ответов)

Как вы считаете, может ли повлиять интернет-активность вашего ребенка на его взгляды на жизнь?

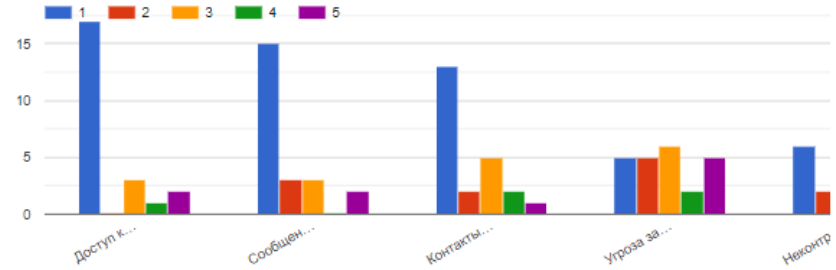
23 ответа



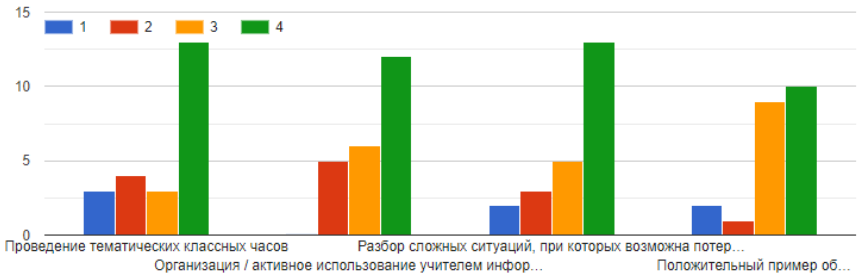
Влияет ли интернет-активность Вашего ребенка на его здоровье?

23 ответа

Какие из существующих интернет угроз, с которыми может столкнуться ребенок, вызывают у Вас наибольшее опасение?Оцените по шкале 1-5 (1 - вызывает наибольшее опасение, 5 – вызывает наименьшее опасение)



Как учителя могут повлиять на воспитание интернет-культуры и усвоение навыков информационной безопасности? *Расставьте в порядке значимости 1 - незначимо, 4 - наиболее значимо*

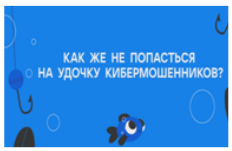


Приложение 2. Памятка по информационной безопасности

Киберпреступники в сетях

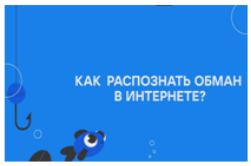
Фишинговые ссылки

1. Просмотреть страничку пользователя
2. Не переходить по незнакомым ссылкам
3. Проверить адресную строку
4. Проверить цену (на Фишинговые сайтах цена необычно низкая)
5. Покупать на проверенных сайтах/в кассе



Социальная инженерия

Социальная инженерия — это разные виды манипуляций и обмана, цель которых заставить человека раскрыть личные данные, получить доступ к его личной и финансовой информации.

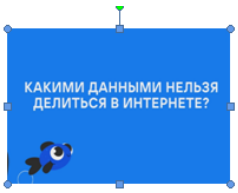


1.Попросить подробно рассказать о себе
2. Проверить, действительно ли такой человек существует

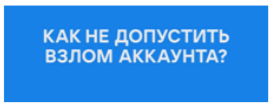
Помните! Мошенники будут торопить вас предоставить информацию!

Защита личной информации

1. Использовать фильтр Для близких людей
2. Не выкладывать личные данные в сеть

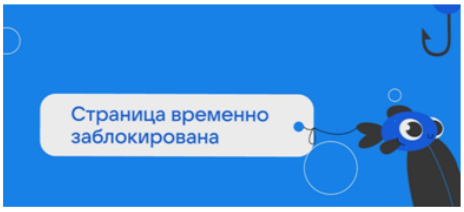


Защита профиля



1. Использовать разные пароли
2. Менять пароль не реже чем один раз в полгода
3. Пароль должен содержать не менее 8 символов (строчные, прописные буквы символы цифры)
4. Подключить дополнительное подтверждение входа.

При подозрении о взломе пожаловаться на запись – модераторы заблокируют страницу



Ситуационный классный час «Кибербуллинг», как формат модели формирования навыков безопасного поведения в сети интернет

Игнатьева Елена Сергеевна,
учитель английского языка
Пивоварова Наталья Сергеевна,
учитель биологии
МБОУ «СОШ № 8 им. Бусыгина М.И.»

Цель: Познакомить учащихся с опасностями в интернете, помочь избежать этих опасностей, профилактика правонарушений в сети. **Слайд 4.**

Задачи: Формирование знаний и умений по защите своих данных в сети интернет, и профилактика правонарушений в сети. **Слайд 5.**

Используемый материал:

Презентация, разработка классного часа для обучающихся 7-8 классов по технологии рефлексивного воспитания Н.П. Капустина

Ожидаемый результат:

Повышение уровня информационных компетенции участников классного часа в области информационной безопасности.

Структура классного часа:

I. Приветствие.

II. Вступление.

III. «Я – позиция» (в круге)

IV. «Я – позиция и общественная норма» (в группе)

V. Дискуссия

VI. Рефлексия. (в круге)

VII. Свободный выбор. **Слайд 7.**

Ход классного часа.

Этапы	**Содержание**
I. Приветствие.	Добрый день, ребята.
II. . Вступление	Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для саморазвития и общения. Но Интернет может быть не только кладезем возможностей, но и источником угроз. Исследования показали: каждого четвертого ребенка в нашей стране унижают и травят в Интернете. просмотр видеоролика https://www.youtube.com/watch?v=VBYeW5JtLWw
Ш.«Я – позиция». (вопрос в круге)	1. Знаете ли вы, что такое кибербулинг? 2. Сталкивались ли вы или ваши знакомые с кибербулингом?

IV. «Я – позиция» и общественно-значимая норма. (в группе)	Предлагаю вам в течение 7-10 минут поработать в группе и ответить на предложенные вам вопросы, пользуясь данными распечатками и своим опытом. **<u>1 группа</u>** «Кибербулинг-прикол или правонарушение? И все-таки, это прикольно или противоправно ? Основной закон Российской Федерации - это Конституция Российской Федерации. Если имел место факт оскорбления личности в социальных сетях, то необходимо знать статьи Конституции РФ, Гражданского кодекса РФ, Уголовного кодекса РФ, Кодекса РФ об административных правонарушениях, гарантирующие права и свободы, содержащие нормы ответственности за нарушение поведения в социуме, которым является и Интернет. В **Конституции** написано … <u>Статья 2</u> Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина - обязанность государства. <u>Статья 18</u> Права и свободы человека и гражданина являются непосредственно действующими. Они определяют смысл, содержание и применение законов, деятельность законодательной и исполнительной власти, местного самоуправления и обеспечиваются правосудием. <u>Статья 21</u> Достоинство личности охраняется государством. Ничто не может быть основанием для его умаления. Никто не должен подвергаться пыткам, насилию, другому жестокому или унижающему человеческое достоинство обращению или наказанию.

	Статья 23 Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. **Гражданский кодекс РФ** Статья 152.1. Охрана изображения гражданина Часть 1. Обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина. **Кодекс Российской Федерации об административных правонарушениях** Статья 5.61. Оскорбление Часть1. Оскорбление, то есть унижение чести и достоинства другого лица, выраженное в неприличной форме, - влечет наложение административного штрафа на граждан в размере от одной тысячи до трех тысяч рублей ; **Уголовный кодекс Российской Федерации** Статья 128.1. Клевета Часть 1. Клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию, наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо обязательными работами на срок до ста шестидесяти часов. Возраст ответственности :Административная ответственность - с 16 лет. Уголовная - по статьям 110, 128.1 и 137 УК РФ - с 16 лет. Материальная ответственность (возмещение вреда): За вред, причиненный

	несовершеннолетним, не достигшим четырнадцати лет (малолетним), отвечают его родители (усыновители) или опекуны, если не докажут, что вред возник не по их вине. *Несовершеннолетние в возрасте от четырнадцати до восемнадцати лет самостоятельно несут ответственность за причиненный вред на общих основаниях*. В случае, когда у несовершеннолетнего в возрасте от четырнадцати до восемнадцати лет нет доходов или иного имущества, достаточных для возмещения вреда, вред должен быть возмещен полностью или в недостающей части его родителями (усыновителями) или попечителем. **2 группа** «Какие чувства испытывает жертва кубербуллинга?» ЖЕРТВЫ КИБЕРБУЛЛИНГА • пугливы, чувствительны, замкнуты и застенчивы; • тревожны, неуверены в себе, несчастны; • склонны к депрессии и чаще своих ровесников думают о самоубийстве; • не имеют ни одного близкого друга. Можно выделить следующие психологические характеристики детей, становящихся жертвами кибербуллинга*:* • Несамостоятельны, легко поддаются влиянию окружающих, безынициативны. • Конформисты, всегда стремятся следовать правилам, неким стандартам (очень прилежны и законопослушны во всем, что касается школьных правил). • Не склонны признавать свою ответственность за происходящее (чаще всего считают виноватыми других).

	• Часто подвержены жесткому контролю со стороны старших (их родители очень требовательны, склонны применять физические наказания). • Эгоцентричны, не умеют ставить себя на место другого. Не склонны задумываться о последствиях своего поведения (в беседах часто говорят:«Я и не подумал об этом»). • Неуверенны в себе, очень дорожат «дружбой», оказанным доверием со стороны лидеров класса (в социометрических исследованиях получают наименьшее количество выборов, нет взаимных выборов ни с кем из класса). • Трусливы и озлоблены. **Следующие симптомы могут свидетельствовать о том, что ребенку плохо в классе, его отвергают.** Ребенок: • неохотно идет в школу и очень рад любой возможности не ходить туда; • возвращается из школы подавленным; • часто плачет без очевидной причины; • никогда не упоминает никого из одноклассников; • очень мало говорит о своей школьной жизни; • не знает, кому можно позвонить, чтобы узнать уроки, или вообще отказывается звонить кому-либо; • ни с того ни с сего (как кажется) отказывается идти в школу; • одинок: его никто не приглашает в гости, на дни рождения, и он никого не хочет позвать к себе. **<u>3 группа</u>** <u>«Как защитить себя от кибербуллинга?»</u>

	1. При общении в Интернете нужно быть дружелюбными с другими пользователями. Ни в коем случае не стоит писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать. 2. Нужно учиться правильно реагировать на обидные слова или действия других пользователей. Лучший способ испортить хулигану его выходку – отвечать ему полным игнорированием. 3. Скрывайте свои страницы в соцсетях Если в соцсети есть приватный режим, то рекомендуем вам применить его на своей странице и общаться исключительно с теми пользователями, которых вы знаете лично в реальной жизни. Вы же не общаетесь с незнакомцами на улице, так зачем делать это онлайн? Часто в интернете люди выдают себя за других, общаясь с ними, вы можете подвергнуть опасности себя и своих близких 4. Помните, что вся личная информация, которую вы выкладываете в Интернете, может быть использована агрессорами против вас. – 5. Поддерживайте доверительные отношения с вашими родителями, они всегда подскажут, как вам поступить в сложной для вас жизненной ситуации. **4 группа** «Что делать, если ты стал жертвой кибербулинга?» 1. Никогда не отвечайте на буллинг Не отвечайте на оскорбительные для вас сообщения, тем более не стоит мстить обидчику ответными сообщениями. Ваши ответные оскорбления или унижение собеседника сделают ситуацию только хуже, а, может быть, приведут к еще большим проблемам.

	2. Делайте скриншоты всех сообщений Если вам прислали сообщение, которое вы считаете оскорбительным для вас, обязательно сделайте его скриншот и сохраните на компьютере – это будет отличным доказательством в будущем. 3. Блокируйте булли и сообщайте администрации ресурса На большинстве ресурсов и во всех соцсетях есть возможность добавить пользователей в черный список, также стоит пожаловаться на пользователя-булли администраторам – его заблокируют, и он не сможет портить жизнь другим участникам ресурса. 4. Поговорите о проблеме с кем-нибудь. Кибербуллинг способен по-настоящему испортить вашу жизнь, хоть вы и не сразу начнете это замечать. Вы не одиноки, не забывайте об этом, поговорите с кем-нибудь о буллинге, близкий человек не только поддержит вас, но и поможет вам собрать доказательства и найти путь выхода из ситуации. 5. Оцените, насколько серьезны угрозы, которые звучат в ваш адрес. Если это пустые слова от пользователя, который вам неизвестен, то и избавиться от него будет легко. Как? Смотрите в пункте 3. Сообщите о булли за пределами сети Если в сети вам угрожает одноклассник, обязательно расскажите об этом учителю и администрации школы. Если кто-то угрожает вам и распространяет ваши персональные данные по всему интернету, сообщите об этом взрослым и в полицию. 6. . Если это возможно, поговорите с обидчиком. Если ваш онлайн-обидчик ходит с вами в одну школу,

	попросите учителя или администрацию заведения побыть судьей между вами. Да, поговорить с булли будет непросто даже психологически, но это принесет большую пользу. Главное, чтобы разговор шел под наблюдением независимого взрослого и по определенным правилам. Проявите сочувствие. Всегда помните, что счастливые и самодостаточные люди не травят других. Булли, как правило, сами находятся в плохом состоянии, поэтому им также нужны помощь и поддержка.
V. Дискуссия	Предлагаю каждой группе ответить на поставленные перед ними вопросы. Ребята из других групп, могут также высказывать свое мнение и дополнять ответы.
VI .Рефлексия (в круге)	Спасибо всем за работу, творческая группа класса оформит общую памятку по кибербуллингу и мы повесим ее в наш классный уголок, а, так же поделимся ею в сети Интернет**.** **Слайд 26.**  **Слайд 27**  Возможно, она будет полезна тем, кто столкнется с этой проблемой. А насколько полезен сегодняшний классный час был для вас? Продолжите, пож-та, одну из этих фраз:

	1. Я сегодня узнал(а)… 2. Оказывается… 3. Я раньше не задумывался (лась)… 4. Всегда нужно помнить…
VI. Свободный выбор	К сожаленью, полностью искоренить кибербуллинг, так же, как другие проявления жестокости в виртуальном пространстве и реальной жизни, невозможно. Но нужно помнить, что только мы сами можем строить свое общение в интернет пространстве так, чтобы оно было приятным, полезны и безопасным**.** «Каждый человек – автор своей жизни. Что посеешь – то и пожнешь. Для меня очевидна одна вещь: ответственность за все, что с тобой происходит, лежит только на тебе – независимо от того, согласен ты с происходящим или нет». *Роберт Дауни (младший)* **(Слайд 28)** 

«Концепция информационной безопасности школьников и педагогические условия ее реализации»

Никитина Людмила Александровна,
учитель английского языка МАОУ СОШ №9.

К О Н Ц Е П Ц И Я информационной безопасности детей: от 2 декабря 2015 г.

I. Общие положения…

II. Основные принципы…

III. Приоритетные задачи государственной политики…

IV. Механизмы реализации государственной политики в области информационной безопасности детей.

V. Ожидаемые результаты

Давайте остановимся немного на К О Н Ц Е П Ц И И.

I. Общие положения.

При разумном и эффективном сотрудничестве общественных и государственных институтов информационные и коммуникационные технологии могут быть ключевыми элементами политики, сохраняющими культуру России, укрепляя нравственные и патриотические принципы и развивающими системы культурного и гуманитарного просвещения. **С 4.**

II. Основные принципы.

Информационная безопасность - это защита ребенка от негативного воздействия информационной продукции и создания условий информационной среды для позитивной социализации и индивидуализации, оптимального социального, личностного, познавательного и физического развития, сохранения психического и психологического здоровья и благополучия, а также формирования позитивного мировосприятия. Государственная политика в области обеспечения информационной безопасности детей основывается на конституционных гарантиях равенства прав и свобод граждан и реализуется в соответствии со следующими принципами **их 12**

обучение детей медиаграмотности;

поддержка творческой деятельности детей в целях их самореализации в информационной среде;

- ✓ ***создание условий для формирования в информационной среде благоприятной атмосферы для детей*** вне зависимости от их социального положения, религиозной и этнической принадлежности;

обеспечение широкого доступа детей к историческому и культурному наследию России через использование современных средств массовых коммуникаций;

воспитание у детей навыков самостоятельного и критического мышления;

- ✓ ***взаимодействие различных ведомств*** при реализации стратегий и программ в части, касающейся обеспечения информационной безопасности детей;

III. Приоритетные задачи государственной политики

Обеспечение информационной безопасности детей возможно исключительно при условии эффективного сочетания государственных и общественных усилий при определяющей роли семьи.

Семья, государство и заинтересованные в обеспечении информационной безопасности детей общественные организации имеют следующие приоритетные задачи:

- ✓ формирование у детей позитивной картины мира и адекватных базисных представлений об окружающем мире и человеке;
- ✓ ценностное, моральное и нравственно-этическое развитие детей;
- ✓ воспитание у детей ответственности за свою жизнь, здоровье и судьбу;
- ✓ усвоение детьми системы семейных ценностей и представлений о семье;
- ✓ удовлетворение и развитие познавательных потребностей, интересов ребенка и исследовательской активности;
- ✓ развитие творческих способностей детей;

- ✓ формирование у детей навыков самостоятельного и ответственного потребления информационной продукции

IV. Механизмы реализации государственной политики в области информационной безопасности детей. Третий вариант имеет значительные преимущества и представляется наиболее эффективным и позволяет добиться желаемого успеха, если учитывает психолого-педагогические и художественно-культурные характеристики информационной продукции.

С10. В настоящий момент доказала свою высокую эффективность существующая система включения (по решению уполномоченных Правительством Российской Федерации) пяти видов особо социально опасной информации, доступ к которой безусловно должен быть запрещен. В Единый реестр доменных имен, внесен список указателей страниц сайтов в сети "Интернет" и сетевыхадресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено.

Усилия семьи, общества и государства должны быть направлены на то, чтобы ребенок с детства привыкал свободно ориентироваться в медиапространстве, умел взаимодействовать с различными источниками информации, не поддавался манипуляциям извне и мог делать самостоятельные выводы о качестве информационных продуктов.

V. Ожидаемые результаты

Создание новой медиасреды, соответствующей следующим характеристикам:

- ✓ увеличение числа детей, разделяющих ценности патриотизма;
- ✓ снижение уровня противоправного и преступного поведения среди детей;
- ✓ формирование у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования "пиратского" контента.

«Некоторые аспекты работы педагогического коллектива МАОУ СОШ №9 по обеспечению информационной безопасности школьников». Вся

информация по информационной безопасности находится на сайте нашей школы.

Организован режим работы в сети Интернет: (нормативно - методическое обеспечение) 1. Разработан и утвержден режим работы кабинетов с компьютерами;

✓ Оформлены уголки безопасности с размещением в них инструкций, упражнений для глаз при работе за компьютером

✓ Систематически происходит ознакомление с Памятками для родителей и учащихся

Организован режим работы в сети Интернет: (организационно – техническое обеспечение)

✓ Проводятся инструктажи по доступу к образовательным ресурсам Интернет;

✓ Установлены программы-фильтры на школьные компьютеры;

Большое внимание уделяется Формированию информационной культуры участников образовательного процесса: Для Учителя: информация о

✓ негативных формах и способах воздействия ИКТ; методы защиты; правила и нормы сетевого этикета; Прохождение курсовой подготовки.

Для Ученика: Программы классных часов и темы бесед на уроках информатики:

✓ 1. «Основы информационной культуры»;2. «Социальная безопасность» с 5-11класс

✓ 3. Классный час по информационной безопасности «Разговоры о важном» со 2-11 кл

✓ **Раздел Плана по профилактике социально-негативных** явлений среди несовершеннолетних на 2022-2023 учебный год «Обеспечение информационной безопасности обучающихся муниципальных образовательных учреждений»

Памятки для родителей и учеников: «Советы по безопасности работы в общедоступных сетях Wi-Fi», «Вопросы кибербезопасности в сети «Интернет» и др.

Условия эффективного формирования информационной безопасности:

- ✓ содержательный компонент - программы занятий для учащихся (система внеклассных мероприятий, направленных на умение выявлять информационную угрозу);
- ✓ направление на эффективность использования методов, приемов и средств проведения занятий с учетом особенностей развития школьников;
- ✓ психолого-педагогические условия, такие как гуманно- ориентированное и доброжелательное взаимодействие педагога и учащихся.

Мы должны помнить, что ИНТЕРНЕТ может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями.

Но – как и реальный мир –

Сеть тоже может быть опасна!