**Локальный акт № 82**

Утверждено
на педагогическом совете школы
28 августа 2023 года

**Программа**
**обучения правилам безопасного поведения в Интернете.**

Проблема обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится все более актуальной в связи с существенным ростом численности несовершеннолетних пользователей. В современных условиях развития общества компьютер стал для ребенка и «другом», и «помощником», и даже «воспитателем», «учителем».

Всеобщая информатизация и доступный, высокоскоростной Интернет уравнял всех жителей больших городов и малых деревень в возможности получить качественное образование. Между тем, существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для детей угрозу. Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не

анализируют степень достоверности информации и подлинность ее источников.

Медиаграмотность определяется в международном праве как грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг.

**Цель работы:**

создать условия для обеспечения информационной безопасности детей и подростков при обучении, организации внеурочной деятельности и свободном использовании современных информационно-коммуникационных технологий (в частности сети Интернет)

**Задачи:**

- формирование и расширение компетентности работников образования в области медиабезопасного поведения детей и подростков;
- формирование информационной культуры как фактора обеспечения информационной безопасности;
- изучение нормативно-правовых документов по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию;
- формирование знаний в области безопасности детей, использующих Интернет;
- организация просветительской работы с родителями и общественностью.

Исходя из полученных данных анкетирования учащихся учебного заведения, Интернет является для них главным образом социальной средой. А значит, здесь они могут встречаться как с друзьями, так и с другими людьми.

Работа с обучающимися ведется в зависимости от возрастных особенностей:
- начальное звено (2-4 класс),
- среднее звено (5-9) класс,
- старшее звено (10-11 класс).

На каждом этапе используются необходимые специальные формы и методы обучения в соответствии с возрастными особенностями.

Для изучения проблемы безопасности в сети Интернет и отношения к ней подростков разрабатываются анкеты, позволяющие проанализировать современную ситуацию в образовательной среде.

**Проводится анкетирование в форме анонимного опроса учащихся**

1.Установлен ли Интернет на вашем домашнем компьютере?
 Да – Нет –
2. Чем вы предпочитаете заниматься в Интернете?
 Поиск информации –  Общаться в социальных сетях - Играть в игры –  Смотреть фильмы –
3. Контролируют ли ваши родители то, как вы используете Интернет?
 Да -  Нет –  Не всегда –
4.Какую информацию нельзя размещать в Интернете?
 Свои увлечения –  Свой псевдоним –  Свой домашний адрес –

**Перечень мероприятий «Безопасный Интернет»**

| № | Наименование мероприятий | Дата проведения | Ответственный | Участники |
|---|---|---|---|---|
| 1. | Уроки безопасности по работе в сети | сентябрь | учитель информатики | 5 класс |
| 2. | Интернет для учащихся 1–5 классов. | сентябрь | учитель информатики. | Классные руководители 1-5 классов |
| 3. | Изучение нормативных документов по организации безопасного доступа к сети Школьные методические Интернет объединения | сентябрь | учитель информатики | Педагогический коллектив Семинар-практикум |
| 4. | Организация и проведение конкурса детских работ «Мой безопасный Интернет». Номинации: «Плакат», «Мои любимые сайты», «Любимые сайты нашей семьи».. | октябрь | учитель информатики<br><br>педагог доп.образования, кл.руководители | Учащиеся 5-11 классов |
| 5. | Классные часы по темам: «Безопасность в сети Интернет» (5-6 кл.), «Развлечения и безопасность в Интернете», «Темная сторона Интернета» (7-8 кл.), «Опасности в Интернете», «Как обнаружить ложь и остаться правдивым в Интернете», «Остерегайся мошенничества в Интернете» (9-11 кл.). | ноябрь-феваль | учитель информатики<br><br>педагог доп.образования, кл.руководители | Учащиеся 5-11 классов. |
| 6. | Игра-путешествие «Весѐлый Интернет» | Декабрь- | Классные | Учащиеся |

| | | | | |
|---|---|---|---|---|
| | (обзор детских сайтов) (1-4 кл.)<br>- Экспресс-опрос «Детки в сетке».<br>- Памятки и буклеты для детей: «Защити себя сам!» (советы детям для безопасного поиска в Интернете), «Безопасный Интернет – детям»,<br>«Интернет-ресурсы для детей» (полезные сайты). | март | руководители 1-4 классов,<br><br>педагог-психолог | 1-4 классов |
| 7. | Беседы, диспуты на уроках информатики: «Безопасность при работе в Интернете»,<br>«О личной безопасности в сети Интернет»,<br>«Сетевой этикет», «Этика сетевого общения » (7-8 классы); «Форумы и чаты в Интернет», «Информационная безопасность сетевой технологии работы» (9-11 классы). | Январь-апрель | учитель информатики.<br><br>педагог-психолог | |
| 8. | Выступление на родительском собрании на тему: «Быть или не быть Интернету в компьютере вашего ребенка?»<br>- Анкетирование «Знают ли родители, с кем общается их ребенок в сети?» | В течение года | Заместитель директора по ВР<br><br>педагог-психолог | |

**Приложение №1**

**Методическая разработка классного часа**
**«Безопасный Интернет» для 5-7 классов.**

**Цель:**
познакомить учащихся с опасностями, которые могут подстерегать их в Интернете и помочь избежать этих опасностей.

**Подготовительная работа**:
классный руководитель проводит опрос учащихся:

- У вас на домашнем компьютере установлен Интернет?
- Что вам больше всего нравится в Интернете?
- Как ваши родители воспринимают ваши занятия в Интернете?

**Оборудование:**
компьютер, проектор, презентация, памятка учащимся

**Ход занятия.**

Учитель: раньше подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. И начать наш классный час я хочу с обработанных данных проводимого опроса. Давайте обратим внимание, что наибольший процент ответов на последний вопрос связан с безопасностью в Интернете. И ваши родители во многом правы! Очень большое внимание при работе с Интернетом необходимо уделять именно вопросам безопасности. И

ответить на вопросы: «Какие опасности подстерегают нас в Интернете?» и
«Как их избежать?» нам поможет этот классный час.

**Вопросы:**

1. «Какие опасности подстерегают нас в Интернете?»
2. Что вы ждете от глобальной сети Интернет?

**Преступники в Интернете.**

Преступники преимущественно устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой. Злоумышленники часто сами там обитают; они стараются привлечь подростка своим вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию.

Обычно они хорошо осведомлены о музыкальных новинках и современны увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты,

сдерживающие молодых людей. Некоторые преступники могут действовать

быстрее других и сразу же заводить сексуальные беседы. Преступники могут также оценивать возможность встречи с детьми в реальной жизни.

**Вредоносные программы.**

К вредоносным программам относятся вирусы, черви и «троянские кони»–

это компьютерные программы, которые могут нанести вред вашему компьютеру и хранящимся в нем данным. Они также могут снижать скорость обмена данными с

Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной сети.

**Интернет-мошенничество и хищение данных с кредитной карты**

В чем состоит мошенничество? Среди Интернет - мошенничеств широкое распространение получила применяемая хакерами техника «phishing», состоящая в том, что в фальшивое электронное письмо включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом может и будет использована с ущербом для пользователя.

**Азартные игры.**

Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. В отличие от игровых сайтов, сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

**Онлайновое пиратство.**

Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом – например, музыки, фильмов, игр или программ – без разрешения правообладателя.

**Интернет - дневники.**

Увлечение веб-журналами (или, иначе говоря, блогами) распространяется со скоростью пожара, особенно среди подростков, которые порой ведут интернет - дневники без разрешения взрослых. Последние исследования оказывают, что сегодня примерно половина всех веб -журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Не секрет, что подробное раскрытие личных данных потенциально опасно.

**Интернет-хулиганство.**

Так же, как и в обычной жизни, в Интернете появились свои хулиганы, которые осложняют жизнь другим пользователям Интернета. По сути, они те же дворовые хулиганы, которые получают удовольствие от хамства, грубости в сторону окружающих.

**Недостоверная информация.**

Интернет предлагает колоссальное количество возможностей для обучения, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной. Пользователи Сети должны мыслить критически, чтобы оценить точность материалов; поскольку абсолютно любой может опубликовать информацию в Интернете.

**Материалы нежелательного содержания.**

К материалам нежелательного содержания относятся: материалы порнографического, ненавистнического содержания, материалы суицидальной направленности, сектантские материалы, материалы с ненормативной лексикой.

**Примечание:**

В период занятия учащимся устраивают музыкальные паузы, забавные игры, физкультминутки (Например, по частушки выполняем упражнения: «Руки на пояс, поднимаем плечи по очереди, голову слегка влево, вправо т.д.).

**Как этих опасностей избежать? Или Добрые советы друга.**

**Преступники в Интернете?**

- Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки.

- Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.

**Вредоносные программы.**

- Никогда не открывайте никаких вложений, поступивших с электронным письмом, за исключением тех случаев, когда вы ожидаете получение вложения и точно знаете содержимое такого файла.

- Скачивайте файлы из надежных источников и обязательно читайте предупреждения об опасности, лицензионные соглашения и положения о конфиденциальности.

- Регулярно устанавливайте на компьютере последние обновления безопасности и антивирусные средства.

**Интернет-мошенничество и хищение данных с кредитной карты.**

- Посещая веб - сайты, нужно самостоятельно набирать в обозревателе адрес веб - сайта или пользоваться ссылкой из «Избранного» (Favorites);

- никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.

- Контролируйте списание средств ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют многие банки.

**Азартные игры.**

- Помните, что нельзя играть на деньги. Ведь, в основном, подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают. Играйте в не менее увлекательные игры, те, которые не предполагают использование наличных или безналичных проигрышей/выигрышей.

**Онлайновое пиратство.**

- Помните! Пиратство, по сути, обычное воровство, и вы, скорее всего, вряд ли захотите стать вором. Знайте, что подлинные (лицензионные) продукты всегда выгоднее и надежнее пиратской продукции. Официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией, чего нельзя сказать о компаниях – распространителях пиратских продуктов, которые преследуют только одну цель – обогатиться и за счет потребителя, и за счет производителя. Лицензионный пользователь программного обеспечения всегда может рассчитывать на консультационную и другую сервисную поддержку производителя, о чем пользователь пиратской копии может даже не вспоминать. Кроме того, приобретая лицензионный продукт, потребитель поддерживает развитие этого продукта, выход новых, более совершенных и удобных версий. Ведь в развитие продукта свой доход инвестирует только официальный производитель.

**Интернет- дневники.**

- Никогда не публикуйте в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения. Никогда не помещайте в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверяйте, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию.

**Интернет-хулиганство**.

- Игнорируйте таких хулиганов. Если вы не будете реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут.

**Недостоверная информация.**

- Всегда проверяйте собранную в Сети информацию по другим источникам.

Для проверки материалов обратитесь к другим сайтам или СМИ – газетам, журналам и книгам.

**Материалы нежелательного содержания.**

- Используйте средства фильтрации нежелательного материала (например, MSN Premium's Parental Controls или встроенные в Internet Explorer®).

- Научитесь критически относиться к содержанию онлайновых материалов и не доверять им.

**Примечание:**

**В конце подводятся итоги классного часа (рефлексия)**

- У вас на столе лежат три картинки. Выберите и положите перед собой ту, которая соответствует вашему настроению.

– Классный час понравился. Узнал что-то новое.
– Классный час понравился. Ничего нового не узнал.
– Классный час не понравился. Зря время потерял.

На память о классном часе учитель подарит каждому памятку по безопасному поведению в Интернете.

**Памятка**

**В Сети ты можешь встретить все, что угодно – от уроков истории и новостей до нелепых картинок. Но не стоит думать, что, раз информация появилась в Интернете, она является достоверной.**

Чтобы разобраться, какой информации в Сети можно**, а какой нельзя доверять, следуй простым советам:**

1. **Относись к информации осторожно**. То, что веб - сайт здорово сделан, еще ни о чем не говорит. Спроси себя: за что этот сайт выступает? В чем меня хотят убедить его создатели? Чего этому сайту недостает? Узнай об авторах сайта: зайди в раздел "О нас" или нажми на похожие ссылки на странице. Узнай, кто разместил информацию. Если источник надежный,

например, университет, то, вполне возможно, что информации на сайте можно доверять.

2. **Следуй правилу трех источников**. Проведи свое расследование и сравни три источника информации прежде, чем решить, каким источникам можно доверять. Не забывай, что факты, о которых ты узнаешь в Интернете, нужно очень хорошо проверить, если ты будешь использовать их в своей домашней работе.

3. **Как предоставлять достоверную информацию?**

Будь ответственным – и в реале, и в Сети. Простое правило: если ты не будешь делать что-то в реальной жизни, не стоит это делать в онлайне.

4. **Не занимайся плагиатом**. То, что материал есть в Сети, не означает, что его можно взять без спроса. Если ты хочешь использовать его - спроси разрешения.

5. **Сообщая о неприемлемом контенте, ты не становишься доносчиком.** Наоборот, ты помогаешь делу безопасности Сети.

6. **Когда ты грубишь в Интернете, ты провоцируешь других на такое** же поведение. Попробуй оставаться вежливым или просто промолчать. Тебе станет приятнее.

7. Все, что ты **размещаешь в Интернете, навсегда останется с тобой –как татуировка.** Только ты не сможешь эту информацию удалить или контролировать ее

использование. Ты ведь не хочешь оправдываться за свои фотографии перед будущим работодателем?

8. **Защищай себя – сейчас и в будущем**. Подумай, прежде чем что-либо разместить в Интернете. И помните, Интернет может быть прекрасным и полезным средством

для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна!