

Утверждаю  
директор школы

П.А.Марков



**ПРОГРАММА**  
**обеспечения информационной безопасности**  
**обучающихся**  
**МОБУ СОШ с.Старокуручево**

Определение информационной безопасности несовершеннолетних в Российской Федерации - это комплекс организационных и правовых средств, регламентирующих права несовершеннолетних в информационной сфере, а также обеспечивающих защиту несовершеннолетних от влияния вредной (негативной) информации, влекущей за собой опасность для их жизни и здоровья, либо могущей причинить вред их нормальному нравственному, духовному, психическому и физическому развитию.

**Целью** Программы является создание безопасной информационно-образовательной среды для обеспечения, сохранения и укрепления нравственного, физического, психологического и социального здоровья обучающихся.

**Задачи Программы:**

1. создание организационно-правовых механизмов защиты обучающихся от распространения информации, причиняющей вред их здоровью и развитию;
2. внедрение систем исключения доступа к информации, несовместимой с задачами гражданского становления детей, а также средств фильтрации и иных аппаратно-программных и технико-технологических устройств;
3. профилактика у детей и подростков Интернет-зависимости, игровой зависимости и правонарушений с использованием информационно-телекоммуникационных технологий, формирование у несовершеннолетних навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде через обучение их способам защиты от вредной информации;
4. информационное просвещение родителей (законных представителей) о возможности защиты детей от информации, причиняющей вред их здоровью и развитию.

Программа направлена на создание условий для обеспечения защиты нравственности и охраны здоровья детей в сфере оборота информации. Реализация ее программных мероприятий будет способствовать:

- проведению единой политики, синхронизированной с федеральными, региональными и муниципальными инициативами, при решении задач информационной безопасности обучающихся;
- развитию в детях способности критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях, распознавать и противостоять негативной информации в социальной жизни, СМИ, Интернет-пространстве и мобильной связи, применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

**Нормативно-правовая основа:**

1. Федеральный закон от 29 декабря 2010 года N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию". С дополнениями и изменениями от 18 декабря 2018 г.
2. Указ Президента РФ № 240 от 29 мая 2017 года «Об объявлении в Российской Федерации 2018-2027гг Десятилетием детства». Раздел X «Безопасное информационное пространство для детей».
3. Федеральный закон от 26 декабря 2012 года №273-ФЗ «Об образовании в Российской Федерации».

## Актуальность создания Программы:

Сегодня информационно-коммуникативные технологии (ИКТ) предоставляют беспрецедентные возможности для детско-юношеского обучения и творчества. Данный потенциал, обладающий информационной насыщенностью и интенсивностью, многоканальностью влияний, многообразием транслируемых ценностей, включает ресурсы открытых цифровых хранилищ библиотек, музеев, федеральных и региональных образовательных коллекций, образовательных сайтов и телеканалов.

В то же время многие ученые, педагоги, родители, общественность серьезно обеспокоены негативным влиянием современной информационной среды на детей и молодежь. К самым распространенным угрозам можно отнести:

- **Угроза заражения вредоносным ПО.** Ведь для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.
- **Доступ к нежелательному содержанию.** Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна содержащие любую информацию, чаще всего порнографического характера;
- **Контакты с незнакомыми людьми с помощью чатов или электронной почты.** Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи;
- **Неконтролируемые покупки.** Не смотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

За последние 20 лет в детской среде произошли серьезные изменения, связанные с неограниченной доступностью СМИ, средств мобильной связи и сети Интернет. По данным социологических опросов дети стали гораздо меньше читать книги и предпочитают пользоваться электронными медиа ресурсами, проводя много времени у компьютера и телевизора. Так, согласно опросам Фонда "Общественное мнение", каждый четвертый подросток ежедневно работает в сети, три четверти подростков (75,5%) входят в состав полугодовой аудитории Интернета. Не пользуются Интернетом лишь менее четверти (24,5%) подростков. Большинство объясняют это объективными трудностями (нет компьютера или доступа в Интернет, не позволяют финансы, просто нет возможности, в том числе в учебном заведении) и лишь некоторые субъективными трудностями (не умею, не хочу, мне это неинтересно). При этом формы проведения досуга, связанные с межличностным общением, сохранили свою значимость на прежнем высоком уровне. Только средства этого общения стали несколько иными (мобильные телефоны, ICQ, социальные сети).

Серьезной и глобально значимой проблемой стало злоупотребление плодами ИКТ и их использование для совершения преступлений против детей, которые особенно уязвимы в условиях интенсивного развития новых информационных технологий (Интернета, мобильной и иных видов электронной связи, цифрового вещания), доступности СМИ, распространения информационно-телекоммуникационных сетей общего пользования, интенсивного оборота рекламной продукции, электронных и компьютерных игр, кино-, видео-, иных аудиовизуальных сообщений и материалов. Их бесконтрольное использование нередко оказывает на детей и подростков психотравмирующее и растлевающее влияние, побуждает их к рискованному, агрессивному, жестокому, антиобщественному поведению, облегчает их вовлечение в криминальную деятельность, развратные действия, азартные игры, тоталитарные секты и иные деструктивные организации.

При этом родители зачастую отстают от информационной грамотности своего ребенка, не подозревая, какой опасности он подвергается, сидя дома за компьютером, какой контент ребенок смотрит по телевидению и видео. Многие не знают и не интересуются содержанием сайтов, которые посещает их ребенок, в какие компьютерные игры играет, какую музыку слушает.

Поскольку большинство современных родителей жалуются на занятость на работе, то для воспитания детей и контроля за их занятиями остается мало времени, сил, а порой и компетентности. Вследствие этого дети и подростки, в силу возраста не обладающие способностью фильтровать качество информации, могут бесконтрольно смотреть любые телепрограммы и посещать небезопасные для детского возраста Интернет-страницы.

Насыщенность современной информационно-образовательной среды при бесконтрольном доступе может быть деструктивной, вредной для обучающихся. В целом на сегодняшний день состояние информационно-образовательной среды можно оценить как небезопасное для ребенка.

В настоящее время регулирование вопросов обеспечения информационной безопасности несовершеннолетних производится неэффективно.

Поэтому при реализации Программы обеспечения информационной безопасности обучающихся необходимо действовать системно, комплексно и использовать не только правовые регуляторы, но и технические и технологические возможности.

#### **Прогноз результатов реализации программы:**

- увеличение доли информированности граждан об имеющихся возможностях защиты обучающихся от информации, причиняющей вред их здоровью и развитию.

#### **Показатели эффективности Программы:**

- охват обучающихся, их родителей, педагогов занятиями по медиа безопасности;
- информированность родителей (законных представителей) об имеющихся возможностях защиты детей от информации, причиняющей вред их здоровью и развитию.

Оценка эффективности реализации Программы производится на основе годовых отчетов.

## ПЛАН МЕРОПРИЯТИЙ

Задача 1: Создание организационно-правовых механизмов защиты детей от распространения информации, причиняющей вред их здоровью и развитию

1.1. Разработка учебных занятий, классных часов с тематикой по защите обучающихся от распространения вредной для них информации.

1.2. Направление педагогических работников на семинары и курсы повышения квалификации по данной проблеме

1.3. Разработка материалов для проведения мероприятий по работе с семьей по проблемам информационной безопасности.

Задача 2: Внедрение систем исключения доступа к информации, несовместимой с задачами гражданского становления детей, а также средств фильтрации и иных аппаратно-программных и технико-технологических устройств.

2.1. Оснащение рабочих мест с доступом к сети Интернет, обслуживающих обучающихся, контентом фильтрации.

2.2. Своевременное заключение договоров с провайдером услуги доступа к сети Интернет-трафика образовательным учреждением с обеспечением контент-фильтрации.

2.3. Информирование родителей (законных представителей) о выявлении фактов распространения материалов порнографического экстремистского содержания и информации о жестокости по отношению к детям и с их стороны, а также экстремистского характера, пропаганды наркотических средств, психотропных веществ или их прекурсоров.

Задача 3: Профилактика у детей и подростков Интернет-зависимости, игровой зависимости и правонарушений с использованием информационно-телекоммуникационных технологий, формирование у несовершеннолетних навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде через обучение их способам защиты от вредной информации.

3.1. Заказ мониторинга информационных потребностей различных категорий обучающихся с целью выработки рекомендаций по совершенствованию информационного обеспечения детей и подростков. Направление аналитической справки заинтересованным органам системы профилактики безнадзорности и правонарушений несовершеннолетних.

3.2. Проведение медиа уроков по теме "Информационная безопасность обучающихся».

3.3. Участие в конкурсах и других мероприятиях для школьников как непосредственно связанных с пропагандой безопасного поведения в сети Интернет, так и вовлекающих детей в безопасное образовательное пространство.

3.4. Участие в конференциях и семинарах для детей, молодежи и специалистов, работающих с детьми и молодежью по Интернет-безопасности.

3.5. Проведение разъяснительных профилактических мероприятий с несовершеннолетними и их родителями об ответственности за распространение информации экстремистского, порнографического и наркотического характера.

3.6. Организация помощи родителям по обращению в учреждения социального обслуживания, включающих вопросы оказания психолого-педагогической помощи семьям несовершеннолетних с Интернет-зависимостью.

3.7. Размещение на официальном сайте образовательного учреждения ссылок на электронные адреса для направления информации о противоправном Интернет-контенте.

3.8. Размещение на официальном сайте образовательного учреждения материалов для родителей по тематике обеспечения информационной безопасности детей.