



Муниципальное казенное общеобразовательное учреждение «Средняя общеобразовательная школа №7» Левокумского муниципального округа Ставропольского края

Центр образования естественно-научной и технологической направленностей
«Точка роста»

СОГЛАСОВАНО

Руководитель Центра образования
естественно-научной
и технологической направленности
 /Емельянова Л.В./

УТВЕРЖДАЮ

Директор МКОУ СОШ №7
 /Т.В.Кузнецова/
Приказ №183-од от 30.08.2024г.



Рабочая программа
курса внеурочной деятельности
«Безопасность в сети Интернет»
технологической направленности
Возраст обучающихся – 10-12 лет
Срок реализации – 1 год

Составитель программы:
учитель математики и информатики
высшей квалификационной категории
Заворотынская
Татьяна Владимировна

с.Величаевское,
2024-2025 уч. год

Пояснительная записка

Рабочая программа курса внеурочной деятельности «Безопасность в сети Интернет» построена на основе:

1. Закон «Об образовании в Российской Федерации» № 273-ФЗ от 29.12.2012г.;
2. Приказ Минпросвещения России от 31.05.2021 N 287 "Об утверждении федерального государственного образовательного стандарта основного общего образования»;
3. Методические рекомендации по созданию и функционированию в общеобразовательных организациях, расположенных в сельской местности и малых городах, центров образования естественно-научной и технологической направленностей (письмо Министерства просвещения Российской Федерации от 30.11.2023 г. №ТВ-2356/02).
4. Приказ МКОУ СОШ №7 № 51-од от 05.04.2024г. «О создании центра образования естественно-научной и технологической направленностей «Точка роста»
5. Положение МКОУ СОШ №7 о Центре естественно-научной и технологической направленностей «Точка роста» (утверждено приказом № 51-од от 05.04.2024г.).

Актуальность

Безопасность в информационном обществе является одним из основных направлений фундаментальных исследований в области информационных технологий.

Компьютерные технологии применяются при изучении практически всех школьных дисциплин уже с младших классов, поэтому, как указано в «Стратегии развития отрасли информационных технологий в Российской Федерации»: «Необходимо совершенствовать современную профессиональную подготовку учителей информатики и преподавателей дисциплин в сфере информационных технологий», а значит, и в сфере кибербезопасности. Киберугрозы существуют везде, где применяются информационные технологии, следовательно, преподаватель любой дисциплины может в профессиональной деятельности столкнуться и со спамом, и с вирусами, и со взломом компьютера и с многими другими проблемами, на которые нужно не только оперативно реагировать, но и насколько возможно уметь предотвращать их появление, а значит, постоянно упоминать в контексте урока различные аспекты организации информационной безопасности

Цель программы:

формирование у учащихся навыков безопасного поведения в медиапространстве и профилактика негативного влияния современных IT-технологий на психику школьников.

Ключевыми понятиями рассмотрения данной проблемы являются понятия информационно-психологическая безопасность, психическое здоровье, психологическая безопасность личности.

Задачи обучения:

1. познакомить школьников с нормативно-правовыми документами по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию;
2. сформировать знания в области медиабезопасности детей, использующих Интернет, СМИ, различные виды телекоммуникаций;
3. ознакомить с технологиями и средствами защиты информации;
4. сформировать у учащихся навыки по профилактике и коррекции зависимого поведения, связанного с компьютерными технологиями и Интернетом.

Объем программы

Программа рассчитана на 1 год обучения. На реализацию курса отводится 36 занятий (по 3 часа в неделю), 108 часов в год.

Возраст обучающихся – 10-12 лет

Планируемые результаты освоения курса «Безопасность в сети Интернет» в 5-6 классах

Предметными результатами: усвоение учащимися конкретных элементов социального опыта, знаний, умений и навыков, опыта решения проблем, опыта творческой деятельности, которые необходимы для самореализации в пределах интернета.

Метапредметные результаты: освоенные обучающимся способы деятельности, применимые как в рамках образовательного процесса, так и при решении проблем социального характера в реальных жизненных ситуациях. Личностные результаты должны отразиться в формировании системы ценностных отношений обучающихся к себе и окружающим, самому образовательному процессу и его результатам.

Требования к результатам обучения:

После успешного изучения и практической работы в Программе учащиеся смогут:

1. осознать значимость проблемы медиабезопасности детей и подростков, ее решение для развития общества и будущего подрастающего поколения;
2. сформировать компетенции в области правовых аспектов медиабезопасности детей и подростков;
3. освоить способы защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи.

Содержание учебного курса

Модуль 1. Информационно-психологическая безопасность личности в изменяющемся обществе. Психическое здоровье как ценность. (18 ч.)

Тема 1.1. Информационно-психологическая безопасность личности

Информационно-психологическая безопасность (ИПБ) как научно-практическое направление, созданное в целях обеспечения защищенности отдельной личности от противоправных информационных воздействий и создания информационной сферы.

Тема 1.2. Психологическая защищенность личности и информационно-психологическая безопасность

Психологическая защита личности как многоуровневая система социальных, социально-психологических и индивидуально-личностных механизмов, образований и форм поведения, обеспечивающая информационно-психологическую безопасность человека в обществе. Психологическая защищенность в условиях действия многообразных информационных факторов и в различных информационно-коммуникативных ситуациях.

Три основных уровня организации психологической защищенности человека:

- 1) социальный (в масштабах общества в целом);
- 2) социально-групповой (в рамках различных социальных групп);
- 3) индивидуально-личностный.

Модуль 2. Сохранение физического и психического здоровья детей в современной информационной среде. (18 ч.)

Тема 2.1. Здоровьесберегающие технологии при работе на ПК

Здоровьесберегающие технологии, применяемые при организации работы школьника на компьютере. Гигиенические требования к организации занятий с использованием новых информационно-компьютерных технологий. Профилактика нарушений здоровья детей в современной информационной среде.

Тема 2.2. Негативное воздействие компьютера на психическое здоровье детей

Воздействие компьютера на психическое здоровье детей. Уход от реальности. Признаки, характерные для игромании как разновидности зависимого поведения. Стресс при работе с компьютером. Способы его профилактики и коррекции.

Модуль 3. Информационная этика и правовые аспекты защиты информации.

Проблемы взаимодействия IT-технологий и развития личности. (15 ч.)

Тема 3.1. Информационная этика и право

Информационная безопасность. Угрозы информационной безопасности. Уровни информационной безопасности. Направления защиты компьютерной информации.

Тема 3.2. Основные законы России в области компьютерного права и защиты детей.

Ознакомление с нормативно-правовой базой защиты пользователей информационно-коммуникативными средствами:

- Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» (от 29.12.2010 г. № 436-ФЗ –1 с последующим изменением и дополнением);
- Федеральный закон «О связи» (от 07.07.2003 г. № 126-ФЗ с последующим изменением и дополнением);
- Федеральный закон «Об информации, информационных технологиях и защите информации» (от 27.07.2006 г. № 149-ФЗ).

Модуль 4. Безопасность детей, использующих Интернет, мобильную связь, СМИ, различные виды телекоммуникаций. (24 ч.)

Тема 4.1. Опасности, с которыми дети могут столкнуться в сети Интернет. Организация правильного поиска необходимой информации в сети Интернет и СМИ

Риск получения ребенком доступа к неподходящей информации. Типы рисков. Организация правильного поиска необходимой информации в сети Интернет и СМИ.

Тема 4.2. Безопасное общение детей в Интернете

Противостояние угрозам из Интернета. Инструкции по безопасному общению в чатах. Интернет-этика поведения в Интернете. Как не следует вести себя в Сети. Безопасное общение при использовании мобильной (сотовой) связи.

Тема 4.3. Компьютерная атака. Феномен «Интернет-зависимости». Профилактика Интернет-зависимости у детей и подростков.

Феномен «Интернет-зависимости». Профилактика Интернет-зависимости. Преодоление Интернет-зависимости у детей и подростков.

Тема 4.4. Технологии безопасной работы в сети Интернет

Основные угрозы безопасности детей в Интернете: киберхулиганы, злоупотребление общим доступом к файлам, хищники, неприличный контент, вторжение в частную жизнь. Повышение уровня общей безопасности при работе в сети. Советы по безопасности при работе на общедоступном компьютере.

Модуль 5. Технологии и средства защиты информации от противоправных посягательств в сети Интернет, мобильной (сотовой) связи и СМИ. (18 ч.)

Тема 5.1. Уровни и меры по защите информации

Цели совершения преступления. Основные понятия в области защиты информации от разрушения и несанкционированного доступа. Уровни защиты информации. Меры по защите информации. Планирование мер по защите информации на создаваемые электронные ресурсы.

Тема 5.2. Меры безопасности при работе с электронной почтой

Основные угрозы личной безопасности: кража идентификационных сведений, мистификация, нежелательная почта (спам). Доступ к файловой системе (папкам). Утечка информации через электронную почту. Меры безопасности при работе с электронной почтой.

Тема 5.3. Основы безопасности сотовой (мобильной) связи

Основы безопасности при использовании мобильной (сотовой) связи. Виды мошенничества в мобильной связи. Меры предосторожности и безопасности при использовании сотовой (мобильной) связи.

Модуль 6. Компьютерные вирусы и средства защиты. (9 ч.)

Обзор и классификация компьютерных вирусов. Способы распространения вирусов. История вредоносных программ. Вирусная терминология. Классификация вирусов. Самые распространенные вирусы. Цикл функционирования вирусов. Антивирусное программное обеспечение и антишпионские программы.

Методы борьбы с вирусами. Меры защиты от проникновения и распространения вирусов.

Повторение пройденного материала (3 ч.)

Тематическое планирование

| № п/п | Наименование модулей, разделов, форм работы | Всего часов | В том числе: | |
|-------|---|-------------|--------------|-----------|
| | | | Теория | Практика |
| 1 | Модуль 1. Информационно-психологическая безопасность личности в изменяющемся обществе. Психическое здоровье как ценность. | 18 | 12 | 6 |
| 2 | Модуль 2. Сохранение физического и психического здоровья детей в современной информационной среде. | 18 | 9 | 9 |
| 3 | Модуль 3. Информационная этика и правовые аспекты защиты информации. Проблемы взаимодействия ИТ-технологий и развития личности. | 15 | 9 | 6 |
| 4 | Модуль 4. Безопасность детей использующих Интернет, СМИ, различные виды телекоммуникаций. | 24 | 15 | 9 |
| 5 | Модуль 5. Технологии и средства защиты информации от противоправных посягательств в сети Интернет, мобильной (сотовой) связи и СМИ. | 18 | 9 | 9 |
| 6 | Модуль 6. Компьютерные вирусы и средства защиты | 12 | 9 | 3 |
| 7 | Итоговое повторение | 3 | 1 | 2 |
| | Итого по курсу: | 108 | 64 | 44 |

Календарно – тематическое планирование курса

| № п/п | № в теме | Название темы | Тип занятия | Дата | | Примечание |
|---|-------------|---|----------------|----------|----------|------------|
| | | | | по плану | по факту | |
| Модуль 1. Информационно-психологическая безопасность личности в изменяющемся обществе. Психическое здоровье как ценность 18ч | | | | | | |
| 1 2 3 4 | 1 | Информационно-психологическая безопасность личности. | Теория | | | |
| 5 6 | 2 | Информационно-психологическая безопасность (ИПБ) как научно-практическое направление. | Практика | | | |
| 7 8 9 10 | 3 | Защищенность отдельной личности от противоправных информационных воздействий и создания информационной сферы. | Теория | | | |
| 11 12 | 4 | Психологическая защищенность личности и информационно-психологическая безопасность. | Практика | | | |
| 13 14 | 5 | Психологическая защищенность в условиях действия многообразных информационных факторов и в различных информационно-коммуникативных ситуациях. | Практика | | | |
| 15 16 17 18 | 6 | Три основных уровня организации психологической защищенности человека. | Теория | | | |
| Модуль 2. Сохранение физического и психического здоровья детей в современной информационной среде , 18ч | | | | | | |
| 19 20 21 | 1 | Здоровьесберегающие технологии, применяемые при организации работы школьника на компьютере. | Теория | | | |
| 22 23 24 | 2 | Гигиенические требования к организации занятий с использованием новых информационно-компьютерных технологий. | Теория | | | |
| 25 | 3 | Профилактика нарушений здоровья детей в современной информационной среде. | Теория | | | |

| | | | | | |
|---|---|---|----------|--|--|
| 26 | | | | | |
| 27 | | | | | |
| 28 | 4 | Воздействие компьютера на психическое здоровье детей. Уход от реальности. | Практика | | |
| 29 | | | | | |
| 30 | | | | | |
| 31 | 5 | Признаки, характерные для игромании как разновидности зависимого поведения. | Практика | | |
| 32 | | | | | |
| 33 | | | | | |
| 34 | 6 | Стресс при работе с компьютером. Способы его профилактики и коррекции. | Практика | | |
| 35 | | | | | |
| 36 | | | | | |
| Модуль 3. Информационная этика и правовые аспекты защиты информации. Проблемы взаимодействия IT-технологий и развития личности , 15ч | | | | | |
| 37 | 1 | Информационная этика и право. | Теория | | |
| 38 | | | | | |
| 39 | | | | | |
| 40 | 2 | Информационная безопасность. Угрозы информационной безопасности. | Теория | | |
| 41 | | | | | |
| 42 | | | | | |
| 43 | 3 | Уровни информационной безопасности. Направления защиты компьютерной информации. | Практика | | |
| 44 | | | | | |
| 45 | | | | | |
| 46 | 4 | Проблемы взаимодействия IT-технологий и развития личности. | Практика | | |
| 47 | | | | | |
| 48 | | | | | |
| 49 | 5 | Основные законы России в области компьютерного права и защиты детей. | Теория | | |
| 50 | | | | | |
| 51 | | | | | |
| Модуль 4. Безопасность детей, использующих Интернет, мобильную связь, СМИ, различные виды телекоммуникаций , 24ч | | | | | |
| 52 | 1 | Риск получения ребенком доступа к неподходящей информации. Типы рисков. | Теория | | |
| 53 | | | | | |

| | | | | | |
|---|---|--|----------|--|--|
| 54 | | | | | |
| 55 56 57 | 2 | Организация правильного поиска необходимой информации в сети Интернет и СМИ. | Практика | | |
| 58 59 60 | 3 | Противостояние угрозам из Интернета. Инструкции по безопасному общению в чатах. | Теория | | |
| 61 62 63 | 4 | Интернет-этика поведения в Интернете. Как не следует вести себя в Сети. | Теория | | |
| 64 65 66 | 5 | Безопасное общение при использовании мобильной (сотовой) связи. | Практика | | |
| 67 68 69 | 6 | Феномен «Интернет-зависимости». Профилактика Интернет-зависимости. Её преодоление у детей и подростков. | Теория | | |
| 70 71 72 | 7 | Основные угрозы безопасности детей в Интернете: киберхулиганы, злоупотребление общим доступом к файлам, хищники, неприличный контент, вторжение в частную жизнь. | Практика | | |
| 73 74 75 | 8 | Повышение уровня общей безопасности при работе в сети. Советы по безопасности при работе на общедоступном компьютере. | Теория | | |
| Модуль 5. Технологии и средства защиты информации от противоправных посягательств в сети Интернет, мобильной (сотовой) связи и СМИ , 18ч | | | | | |
| 76 77 78 | 1 | Цели совершения преступления. Основные понятия в области защиты информации от разрушения и несанкционированного доступа. | Теория | | |
| 79 80 81 | 2 | Уровни защиты информации. Меры по защите информации. Планирование мер по защите информации на создаваемые электронные ресурсы. | Теория | | |
| 82 | 3 | Основные угрозы личной безопасности: кража идентификационных сведений, мистификация, | Практика | | |

| | | | | | | |
|---|---|--|--------------------|--|--|--|
| 83 84 | | нежелательная почта (спам). Доступ к файловой системе (папкам). | | | | |
| 85 86 87 | 4 | Утечка информации через электронную почту. Меры безопасности при работе с электронной почтой. | Теория | | | |
| 88 89 90 | 5 | Основы безопасности при использовании мобильной (сотовой) связи. Виды мошенничества в мобильной связи. | Практика | | | |
| 91 92 93 | 6 | Меры предосторожности и безопасности при использовании сотовой (мобильной) связи. | Практика | | | |
| Модуль 6. Компьютерные вирусы и средства защиты , 12 ч | | | | | | |
| 94 95 96 97 | 1 | Обзор и классификация компьютерных вирусов. Способы распространения вирусов. История вредоносных программ. | Теория | | | |
| 98 99 100 101 | 2 | Методы борьбы с вирусами. Меры защиты от проникновения и распространения вирусов. | Теория | | | |
| 102 103 | 3 | Методы борьбы с вирусами. Меры защиты от проникновения и распространения вирусов. | Практика | | | |
| 104 105 | 4 | Методы борьбы с вирусами. Меры защиты от проникновения и распространения вирусов. | Практика | | | |
| Итоговое повторение, 3ч | | | | | | |
| 106 107 108 | | Повторение пройденного материала. | Теория Практика | | | |

**Учебно-методическое и материально-техническое обеспечение
образовательного процесса**

1. Основы безопасности, Тонких И.М., Москва, 2016
2. Сайт «Сетевичок.рф»
3. [http://nto.immpu.sgu.ru/site\\$/default/files/3/I2697.pdf](http://nto.immpu.sgu.ru/site$/default/files/3/I2697.pdf)