бюджетное общеобразовательное учреждение
Сокольского муниципального округа
«Средняя общеобразовательная школа № 3»

Согласовано
на педагогическом совете
протокол №1
от 29.08.2024 г.

Утверждено
приказ № 120 от 29.08.2024 г.
Директор БОУ СМО «СОШ №3»
_____С.А.Хвалина

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

технической направленности

« Информационная безопасность"

Возраст обучающихся 13-17 лет

Срок реализации -12 часов (краткосрочная)

Сокол

2024 г.

Пояснительная записка

Огромные массивы информации обрушиваются на человека ежедневно через газеты и журналы, радио и телевидение, всевозможную рекламу.

Психологи все чаще употребляют термин “сжатие миром”. Плотной стеной мир обступает почти каждого из нас, вынуждая воспринимать информацию вне зависимости от возможностей и желания. Порой информация помогает нам ориентироваться в современном мире, а иногда утомляет и мешает принять правильное решение.

Защита человека от поступающей к нему информации является важнейшей составляющей обеспечения его личной безопасности. Человек должен уметь защищаться от возможных информационных манипуляций.

В условиях информатизации общества высокая информационная культура, обеспечивающая информационную безопасность личности, является необходимостью для успешной деятельности в любой сфере.

Теоретически человек сам может переработать любую информацию, но сделает это гораздо эффективнее, если овладеет знаниями и умениями, которыми располагает информационная культура. Поэтому существует острая потребность общества в организации информационного образования, призванного обеспечить формирование информационной культуры и информационной безопасности личности и общества в целом.

Формируя информационную безопасность личности необходимо выработать систему противодействия, защиты личности от возможных информационных манипуляций, а также воспитать чувство ответственности за производство и распространение информации, понимание ее последствий, ее негативного влияния на личность и общество.

Актуальность проблемы воспитания информационной культуры, информационной безопасности обусловлена необходимостью получения знаний, навыков и умений, которыми должен владеть каждый человек в современном, изменяющемся информационном мире. Только личность со сформированной информационной культурой может адекватно реагировать на происходящие в

мире процессы. В условиях информатизации общества, всех его структур, высокая информационная культура, обеспечивающая информационную безопасность личности, является необходимостью для успешной деятельности в любой сфере.

Новизна программы состоит в том, что рассматриваются вопросы информационной безопасности, которая является одной из составляющих безопасности личности, а также вопросы информационной культуры личности, которая способствует реальному пониманию человеком самого себя, своего места и роли в окружающем мире.

Элективный курс «Информационная безопасность» разработан для расширения кругозора и формирования мировоззрения учащихся, повышения уровня безопасности человека в окружающей его информационной среде.

Предложенный материал дополняет образовательные области ОБЖ и информатика, способствует воспитанию информационной культуры обучающихся, формированию информационной безопасности личности, созданию условий для повышения готовности подростков к сознательному, профессиональному и культурному самоопределению в целом.

Цель программы: обеспечение условий для профилактики негативных тенденций в информационной культуре обучающихся, повышения защищенности детей от информационных рисков и угроз; формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

- ✓ сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
- ✓ создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;

- ✓ сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
- ✓ сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- ✓ сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Планируемые результаты обучения

Предметные

Обучающийся научится:

- ✓ анализировать доменные имена компьютеров и адреса документов в интернете;
- ✓ безопасно использовать средства коммуникации,
- ✓ безопасно вести и применять способы самозащиты при попытке мошенничества,
- ✓ безопасно использовать ресурсы интернета.

Обучающийся овладеет:

- ✓ приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Обучающийся получит возможность овладеть:

- ✓ основами соблюдения норм информационной этики и права;
- ✓ основами самоконтроля, техниками работы с манипуляциями, поддерживая культуру безопасности в сети;
- ✓ использовать для решения коммуникативных задач различные источники информации, включая Интернет-ресурсы и другие базы данных. соблюдать нормы информационной этики и права.

Метапредметные

Регулятивные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- ✓ идентифицировать собственные проблемы и определять главную проблему;
- ✓ выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;

- ✓ ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- ✓ выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- ✓ составлять план решения проблемы (выполнения проекта, проведения исследования);
- ✓ описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- ✓ оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- ✓ находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- ✓ работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- ✓ принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- ✓ выделять явление из общего ряда других явлений;
- ✓ определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
- ✓ строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
- ✓ излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- ✓ самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- ✓ критически оценивать содержание и форму текста;
- ✓ определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- ✓ строить позитивные отношения в процессе учебной и познавательной деятельности;
- ✓ критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;

- ✓ договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- ✓ делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.
- ✓ целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- ✓ выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
- ✓ использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
- ✓ использовать информацию с учетом этических и правовых норм;
- ✓ создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Личностные

- ✓ осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
- ✓ готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- ✓ освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- ✓ сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Срок реализации программы.

Срок реализации 1 год, программа рассчитана на 12 часов. Режим занятий – 12 раз в год по 1 часу (2 раза в месяц по 1 часу). Количество обучающихся в группе 15 человек.

Форма обучения – очная.
Уровень – базовый.
Данная программа предполагает обучение детей в возрасте от 13 до 17 лет.
Для эффективного процесса используются следующие **формы обучения**:

- интегрированные занятия;
- интерактивные игры;
- занятия с применением проектной деятельности.

Периодичность оценки результатов программы
Для оценки уровня освоения дополнительной общеобразовательной программы проводится посредством **текущего контроля, промежуточной аттестации.**
Текущий контроль выявляет степень сформированности практических умений и навыков обучающихся в выбранном ими виде деятельности. Текущий контроль может проводиться в форме наблюдения, индивидуальное собеседование, групповая беседа, опрос.
Текущий контроль осуществляется без фиксации результатов.
Промежуточная аттестация проводится с целью установления уровня (высокий, средний, ниже среднего) освоения отдельной части или всего объёма дополнительной общеобразовательной программы.
-высокий – программный материал усвоен учащимся полностью, учащийся имеет высокие достижения;
-средний – усвоение программы в полном объеме, при наличии несущественных ошибок;
-ниже среднего – усвоение программы в неполном объеме, допускает существенные ошибки в теоретических и практических заданиях.
Формы промежуточной аттестации обучающихся: тестирование, выполнение практического задания, защита проекта.
Итоговый контроль – это промежуточная аттестация, которая проводится по завершению всего объёма дополнительной общеобразовательной программы, которая проводится в следующих формах: тестирование, доклад, защита творческих работ и проектов, итоговое мероприятие.

Способы определения результативности:

- Практические задания.
- Самостоятельные творческие, проектные работы,
- Выставки, конкурсы.
- Работы – участники конкурсов, выставок, документы – свидетельства, дипломы с выставок и т.д.).

УЧЕБНЫЙ ПЛАН

№ п/п	Наименование темы	Количество часов			Формы контроля (аттестации)
		Всего	Теория	Практика	
1.	Общение в социальных сетях и мессенджерах	**2**	**2**	**-**	**Текущий контроль**
2.	Публикация информации в социальных сетях	**2**	**2**	**-**	**Текущий контроль**
3.	Безопасность при введении личных данных	**2**	**2**	**-**	**Текущий контроль**
4.	Резервное копирование данных, вредоносные коды	**2**	**2**	**-**	**Текущий контроль**
5.	Фейки и мнения. Как отличить?	**1**	**-**	**1**	**Промежуточная аттестация**
6.	Информационные ловушки	**1**	**1**	**-**	**Текущий контроль**
7.	Как работать с первоисточником	**1**	**-**	**1**	**Текущий контроль**
8.	Итоговая игра-тестирование	**1**	**-**	**1**	**Итоговый контроль**
	Всего:	**12**	**9**	**3**	

Содержание программы.

В преподавании курса «Информационная безопасность» могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат.

Содержание программы курса соответствует темам основной

образовательной программы основного общего образования (ООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность информации», «Восприятие и работа с информацией».

Каждый раздел курса внеурочной деятельности завершается выполнением проверочного мини-теста.

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. С кем безопасно общаться в интернете. Социальная инженерия: распознать и избежать. 2 часа.

Тема 2. Публикация информации в социальных сетях. Кибербуллинг. Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. Лживые страницы и лживая информация. Овершеринг. 2 часа.

Раздел 2. «Безопасность информации»

Тема 1. Безопасность при введении личных данных. Использовании платежных карт, покупки в Интернете. Пароли для аккаунтов социальных сетей. Безопасный вход в аккаунты. Фишинговые страницы. Режим инкогнито. 2 часа.

Тема 2. Резервное копирование данных, вредоносные коды. Вирусы и антивирусы, способы создать и запомнить пароль, как сохранить информацию. 2 часа.

Раздел 3. «Восприятие и работа с информацией»

Тема 1. Фейки и мнения. Как отличить? Использование эмоций и смайлов в сообщении. Как в эмоциональном сообщении читать факты. Как из факта сделать мнение, игра. 1 час

Тема 2. Информационные ловушки. Интерпретации к фактам. Манипуляция на эмоции. Как останавливать манипуляцию. 1 час.

Тема 3. Как работать с первоисточником. Технология поиска первоисточника. Игра в глухой телефон. 1 час

Тема 4. Итоговая игра-тестирование. Правда или ложь. Этическая задача. 1 час.

Итог: 12 часов.

Календарный учебный график.

Продолжительность реализации программы – в течение одного учебного года.

Режим занятий – 1 час два раза в месяц (1 час в две недели)

Сроки проведения промежуточной аттестации – февраль месяц.

Форма организации деятельности: индивидуальные и групповые занятия с обучающимися.

№ п/п	месяц	Название раздела	Количество часов			Формы аттестации/контроля
			Всего	Теория	Практика	
1	октябрь - апрель	Информационная безопасность	**12**	**3**	**9**	Опрос, практические задания, тест

Раздел №2. Комплекс организационно-педагогических условий

Материально-технические условия реализации

Для реализации ДОП необходимо следующее оборудование:

№ п/п	Наименование материальных ценностей	Единица измерения	Количество
1.	Ноутбук тип 2	шт	1
2.	Ноутбук тип 2	шт	1
3.	Ноутбук тип 2	шт	1
4.	Ноутбук тип 2	шт	1
5.	Ноутбук тип 2	шт	1
6.	Ноутбук тип 2	шт	1
7.	Ноутбук тип 2	Шт.	1
8.	Ноутбук тип 2	Шт.	1
9.	Ноутбук тип 2	Шт.	1
10.	Ноутбук тип 2	Шт.	1
11.	Ноутбук тип 2	Шт.	1
12.	Ноутбук тип 2	Шт.	1
13.	Ноутбук тип 2	Шт.	1
14.	Комплект мебели ученической (стол и стул)	Комплект	12

15.	Комплект мебели учителя (стол и стул)	комплект.	1
16.	Мышки компьютерные	Шт.	20
17.	Моноблочное интерактивное устройство в комплекте с напольной стойкой	Комплект	1
18.	Флип- чарт	Шт.	1
19.	Магнитная доска	Шт.	1

Воспитательный компонент

Программа направлена на повышение уровня информационной безопасности детей и молодежи, привлечение внимания родительской и педагогической общественности к проблеме обеспечения безопасности и развития детей и молодежи в информационном пространстве. Занятия направлены на организацию обучения информационной безопасности и цифровой грамотности детей.

Особое место при работе с программой занимает профориентационная деятельность.

Список литературы

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2016. — 136 с.

2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.

3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.

4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016. — 239 с.

5. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2016. — 239 с.

6. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 с.

7. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.

8. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.

Оценочные материалы.

Приложение № 1

Образец

1. Что можно делать на видеохостинге в YouTube?

1. Размещать материалы без согласия их авторов
2. Выражать своё несогласие с мнением другого в уважительной форме
3. Размещать противозаконные, оскорбительные материалы
4. Грубить в комментариях

2. Какой из паролей является надёжным?

1. Alex2001
2. 19032001
3. 12345678
4. Vbif20hjvfyjd01

3. Что НЕ следует делать, если ты столкнулся с троллем в Сети?

1. Игнорировать выпады тролля
2. Заблокировать тролля
3. Проучить или доказать свою правоту
4. Сообщить модераторам сайта

4. Откуда НЕ стоит брать информацию в Интернете для реферата?

1. Сайты средств массовой информации
2. Википедия
3. Электронные библиотеки
4. Сообщества в социальных сетях

5. Что является признаком достоверности информации в Сети?

1. Возможность перепроверить эту информацию в других источниках и на официальных сайтах

2. Правдоподобность информации

3. Качественное оформление информации

4. Грамотное изложение информации

6. Как НЕ стоит себя вести, если вы стали жертвой кибербуллинга?

1. Ничего не делать

2. Заблокировать обидчиков

3. Сообщить родителям (взрослым)

4. Обратиться на Линию помощи «Дети онлайн»

7. Какие данные из нижеперечисленных можно сообщать по электронной почте?

1. Номера банковских счетов (кредитных карт)

2. Секретные слова (ответы) на специальные секретные вопросы, используемые при идентификации вашего аккаунта

3. PIN-коды

4. Ваши имя и фамилию

8. Когда можно доверять письму от неизвестного отправителя?

1. Отправитель ссылается на ваших друзей

2. Отправитель использует логотип авторитетной компании

3. К вам обращаются по имени

4. Никогда нельзя доверять письму от неизвестного отправителя

9. В каком случае нарушается авторское право?

1. При размещении на YouTube собственного видеоролика с концерта какой-либо группы

2. При чтении романа И. Тургенева «Отцы и дети» в Интернете

3. При использовании материалов Википедии для подготовки доклада со ссылкой на источник

4. При просмотре трансляций на официальном сайте телеканала

10. Как защититься от негативного контента?

1. Использовать безопасный поиск Google и безопасный режим на YouTube

2. Установить антивирус

3. Не обращать на него внимания

4. Обратиться к автору негативного контента

11. Какую информацию о себе можно выкладывать в Интернете в открытом доступе?

1. Место работы родителей

2. Номер телефона

3. Домашний адрес

4. О своих интересах

12. Что делать, если вам пришло письмо о том, что вы выиграли в лотерее?

1. Перейти по ссылке в письме, ведь информация может оказаться правдой

2. Написать в ответ разоблачающее письмо мошенникам

3. Связаться с отправителем по телефону

4. Удалить его и заблокировать отправителя

13. Когда можно полностью доверять новым онлайн-друзьям?

1. Поговорив по телефону

2. После длительной переписки

3. После обмена фотографиями

4. Ничего не может дать100 %-ную гарантию того, что онлайн-другу можно доверять

Ответы

1	2	3	4	5	6	7	8	9	10	11	12	13
2	4	3	4	1	1	4	4	1	1	4	4	4