Муниципальное казённое общеобразовательное учреждение
Сосновская средняя школа

Рассмотрено
на заседании ШМО
классных руководителей
протокол № 1
от «30» августа 2023г.

Согласовано
зам. директора по ВР
_____ Кулагиной Т.Н.
30.08.2023г

Утверждено
приказ № 241
от «31» 08 2023
Директор школы _____ Т.В.Захарова

Программа внеурочной деятельности учащихся
«Безопасность в сети Интернет»

Направление: общеинтеллектуальное
Возраст :8 класс
Срок реализации: 1 год

Сосновка 2023г.

I. Планируемые результаты освоения учебного предмета

Ценностные ориентиры:

Изучение информатики вносит значительный вклад в достижение **главных целей основного общего образования**, способствуя:

- ***формированию целостного мировоззрения***, соответствующего современному уровню развития науки и общественной практики за счет развития представлений об информации как важнейшем стратегическом ресурсе развития личности, государства, общества; понимания роли информационных процессов в современном мире;
- ***совершенствованию общеучебных и общекультурных навыков работы с информацией*** в процессе систематизации и обобщения имеющихся и получения новых знаний, умений и способов деятельности в области информатики и ИКТ; развитию навыков самостоятельной учебной деятельности школьников (учебного проектирования, моделирования, исследовательской деятельности и т.д.);
- ***воспитанию ответственного и избирательного отношения к информации*** с учетом правовых и этических аспектов ее распространения, воспитанию стремления к продолжению образования и созидательной деятельности с применением средств ИКТ.

Задача изучения:

- совершенствование школьного образования и подготовки в сфере информационных технологий, а также популяризация профессий, связанных с информационными технологиями.

Цель изучения:

- дать общие представления о безопасности в информационном обществе и на этой основе сформировать понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности.
- ***Воспитательная цель курса*** – формирование на качественно новом уровне культуры умственного труда и взаимодействия с окружающими, ответственного отношения к вопросам безопасности жизнедеятельности.

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

Выделяются задачи:

- обеспечение различных сфер экономики качественными информационными технологиями;
- обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.
- 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. Преподаватель должен иметь представление о современном уровне развития вычислительной техники, информационный сетей, технологий коммуникации и навигации. С учетом роста числа угроз информационной деятельности и стремительного развития информационных технологий представляется необходимым включить в ФГОСы соответствующие требования, что позволило бы органически дополнить образовательный процесс новыми модулями без рассогласования с имеющимися учебными планами. В число требований к результатам подготовки учащихся необходимо включить не только «удовлетворение познавательных интересов, поиск дополнительной информации», знание «технических устройств (в том числе компьютеров)», умение «искать информацию с применением правил поиска (построения запросов) в базах данных, компьютерных сетях, пользоваться персональным компьютером и его периферийным оборудованием; следовать требованиям техники безопасности, гигиены, эргономики и ресурсосбережения при работе со средствами информационных и коммуникационных технологий», но и знание основ кибербезопасности, умения соблюдать требования кибербезопасности в практической деятельности и организовывать безопасность личного информационного пространства.

<u>Личностные результаты:</u>

это сформировавшаяся в образовательном процессе система ценностных отношений учащихся к себе, другим участникам образовательного процесса, самому образовательному процессу, объектам познания, результатам образовательной деятельности. Основными личностными результатами, формируемыми при изучении информатики в основной школе, являются:

- наличие представлений об информации как важнейшем стратегическом ресурсе развития личности, государства, общества;

- понимание роли информационных процессов в современном мире;
- владение первичными навыками анализа и критичной оценки получаемой информации;
- ответственное отношение к информации с учетом правовых и этических аспектов ее распространения;
- развитие чувства личной ответственности за качество окружающей информационной среды;
- способность увязать учебное содержание с собственным жизненным опытом, понять значимость подготовки в области информатики и ИКТ в условиях развития информационного общества;
- готовность к повышению своего образовательного уровня и продолжению обучения с использованием средств и методов информатики и ИКТ;
- способность и готовность к общению и сотрудничеству со сверстниками и взрослыми в процессе образовательной, общественно-полезной, учебно-исследовательской, творческой деятельности;
- способность и готовность к принятию ценностей здорового образа жизни за счет знания основных гигиенических, эргономических и технических условий безопасной эксплуатации средств ИКТ.

Метапредметные результаты

освоенные обучающимися на базе одного, нескольких или всех учебных предметов способы деятельности, применимые как в рамках образовательного процесса, так и в других жизненных ситуациях. Основными метапредметными результатами, формируемыми при изучении информатики в основной школе, являются:

- требование формирования навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права;
- умения использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;
- понимание основ правовых аспектов использования компьютерных программ и работы в Интернете и т.п.
- владение общепредметными понятиями «объект», «система», «модель», «алгоритм», «исполнитель» и др.;

- владение информационно-логическими умениями: определять понятия, создавать обобщения, устанавливать аналогии, классифицировать, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно-следственные связи, строить логическое рассуждение, умозаключение (индуктивное, дедуктивное и по аналогии) и делать выводы;
- владение умениями самостоятельно планировать пути достижения целей; соотносить свои действия с планируемыми результатами, осуществлять контроль своей деятельности, определять способы действий в рамках предложенных условий, корректировать свои действия в соответствии с изменяющейся ситуацией; оценивать правильность выполнения учебной задачи;
- владение основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности;
- владение основными универсальными умениями информационного характера: постановка и формулирование проблемы; поиск и выделение необходимой информации, применение методов информационного поиска; структурирование и визуализация информации; выбор наиболее эффективных способов решения задач в зависимости от конкретных условий; самостоятельное создание алгоритмов деятельности при решении проблем творческого и поискового характера;
- владение информационным моделированием как основным методом приобретения знаний: умение преобразовывать объект из чувственной формы в пространственно-графическую или знаково-символическую модель; умение строить разнообразные информационные структуры для описания объектов; умение «читать» таблицы, графики, диаграммы, схемы и т.д., самостоятельно перекодировать информацию из одной знаковой системы в другую; умение выбирать форму представления информации в зависимости от стоящей задачи, проверять адекватность модели объекту и цели моделирования;
- ИКТ-компетентность – широкий спектр умений и навыков использования средств информационных и коммуникационных технологий для сбора, хранения, преобразования и передачи различных видов информации, навыки создания личного информационного пространства (обращение с устройствами ИКТ; фиксация изображений и звуков; создание письменных сообщений; создание графических объектов; создание музыкальных и звуковых сообщений; создание, восприятие и использование гипермедиа сообщений; коммуникация и социальное взаимодействие; поиск и организация хранения информации; анализ информации).

Предметные результаты:

включают в себя: освоенные обучающимися в ходе изучения учебного предмета умения специфические для данной предметной области, виды деятельности по получению нового знания в рамках учебного предмета, его преобразованию и применению в учебных, учебно-проектных и социально-проектных ситуациях, формирование научного типа мышления, научных представлений о ключевых теориях, типах и видах отношений, владение научной терминологией, ключевыми понятиями, методами и приемами. В соответствии с федеральным государственным образовательным стандартом общего образования основные предметные результаты изучения информатики в основной школе отражают:

- формирование информационной и алгоритмической культуры; формирование представления о компьютере как универсальном устройстве обработки информации; развитие основных навыков и умений использования компьютерных устройств;
- формирование представления об основных изучаемых понятиях: информация, алгоритм, модель – и их свойствах;
- развитие алгоритмического мышления, необходимого для профессиональной деятельности в современном обществе; развитие умений составить и записать алгоритм для конкретного исполнителя; формирование знаний об алгоритмических конструкциях, логических значениях и операциях; знакомство с одним из языков программирования и основными алгоритмическими структурами — линейной, условной и циклической;
- формирование умений формализации и структурирования информации, умения выбирать способ представления данных в соответствии с поставленной задачей — таблицы, схемы, графики, диаграммы, с использованием соответствующих программных средств обработки данных;
- формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

II. Содержание тем учебного предмета

Тема №1. Общие сведения о безопасности ПК и Интернета (5 часов)

1. **Основные вопросы:** Как устроен компьютер и интернет. Как работают мобильные устройства. Угрозы для мобильных устройств. Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные. Безопасный профиль в социальных сетях. Составляет сети, контактов. Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации. Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, без законные тиражирование (воспроизведение). Безопасный серфинг . Безопасные ресурсы для поиска.
2. **Требования к знаниям и умениям:**

Обучающиеся должны знать как устроен компьютер и интернет , как работают мобильные устройства, какие существуют угрозы для мобильных устройств , что такое защита персональных данных, аспекты кибербезопасности, что такое компьютер и информационная безопасность , что такое кибертерроризм и кибервойны , основные угрозы безопасности информации.

Обучающиеся должны уметь защищать свои персональные данные, составлять безопасные сети контактов, своевременно обнаружить проблемы сети, восстанавливать параметры систем.

3. **Тематика практических работ:**

Практическая работа. Составить информационный буклет «Моя безопасная сеть » или сделать групповую газету «Безопасность в Интернет».

Тема №2. Техника безопасности и экология (5 часов)

1. **Основные вопросы:** Правила повеления в компьютерном классе. Техника безопасности при работе с компьютером. Компьютер и мобильные устройства в чрезвычайных ситуациях. Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM). Комплекс упражнений при работе за компьютером. Гигиена при работе с ПК.
2. **Требования к знаниям и умениям:**

Обучающиеся должны знать правила поведения в компьютерном классе, как применяются компьютер и мобильные устройства в чрезвычайных ситуациях, какое влияние оказывает компьютер на зрение, какое воздействие оказывают радиоволны на здоровье человека и окружающую среду.

Обучающиеся должны уметь соблюдать требования ТБ при работе с компьютером, соблюдать гигиенические требования, проводить комплекс упражнений при работе за компьютером.

3. **Тематика практических работ:**

Практическая работа. Создание буклета «Техника безопасности при работе с компьютером».

Тема №3. Проблемы Интернет – зависимости (5 часов)

1. Основные вопросы: ЗОЖ и компьютер. Деструктивная информация в Интернет как ее избежать. Психологическое воздействие информации на человека. Управление личностью через сеть. Интернет и компьютер зависимость (аддикция). Критерии зависимости точки зрения психологов (приоритетность, изменения, настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость. Типы интернет – зависимости (пристрастие к работе с компьютером, зависимость от сетевого общения, сексуальные зависимости).

2. Требования к знаниям и умениям:

Обучающиеся должны знать что такое ЗОЖ, и как влияет компьютер на здоровье, какое психологическое воздействие оказывает информация на личность человека, критерии зависимости, типы интернет - зависимости, как развевается зависимость.

Обучающиеся должны уметь распознавать и избегать деструктивную информацию в Интернете, уметь вовремя выявить Интернет – зависимость и сообщить специалистам.

3. Тематика практических работ:

Практическая работа. «Создание мультимедийной презентации «ПК и ЗОЖ. Организация рабочего места».

Тема №4 . Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (5 часов)

1. Основные вопросы: Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов. Отличия вирусов и закладок. Как распространяются вирусы. Что такое антивирусная защита . Как лечить компьютер .Антивирусные программы для ПК: сканеры , ревизоры и др. Выявление неизвестных вирусов. Защита мобильных устройств. Безопасность при скачивании файлов. Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно – аппаратные меры защиты. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Методы защиты фото и видеоматериалов от копирования в сети. Проверка подлинности (аутентификация) в Интернете. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях. Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей.

2. Требования к знаниям и умениям:

Обучающиеся должны знать типы вирусов, что такое антивирусная защита, антивирусные программы, как лечить компьютер, как защитить мобильные устройства, как защитить фото и видеоматериалов от скачиваний.

Обучающиеся должны уметь распознавать вирусы, пользоваться антивирусными защитными программами, соблюдать меры личной безопасности при сетевом общении.

3. Тематика практических работ:

Практическая работа №1. «Установка антивирусной программы»;

Практическая работа №2. Создание презентации на тему: «Разновидности вирусов. Черви, трояны, скрипты». «Шпионские программы». «Шифровальщики». «Троян – вымогатель в социальной сети «ВКонтакте» или наказание для особо любопытных».

Тема №5 Мошеннические действия в Интернете. Киберпреступления (5 часов)

1. Основные вопросы: Виды интернет – мошенничества (письма, реклама, охота за личными данными и т. п.). Фишинг (фарминг). Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды. Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса. Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС. Прослушивание разговоров. Определение местоположения телефона. Азартные игры. Онлайн – казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею. Технологии манипулирования в Интернете. Техника безопасности при интернет – общении.

2. Требования к знаниям и умениям:

Обучающиеся должны знать: виды интернет – мошенничества, опасности мобильной сети, технику безопасности при регистрации на веб – сайтах, сайтах знакомств, понятия компьютерное пиратство, плагиат, кибернаемники и кибердетективы.

Обучающиеся должны уметь обезопасить себя при интернет – общении.

3. Тематика практических работ:

Практическая работа. Доклад на тему: «Правила поведения в сети с мошенниками и злоумышленниками», или «Как не стать жертвой сетевых шуток и розыгрышей».

Тема №6 Сетевой этикет. Психология и сеть (5 часов)

1. **Основные вопросы:** Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах. как появился этикет, что это такое. Сетевой этикет. Общие правила сетевого этикета. Этика дискуссий. Взаимное уважение при интернет – общении. Этикет и безопасность. Эмоции в сети, их выражение. Примеры этических нарушений. Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик,смайлики и др. Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид. Если вы стали жертвой компьютерной агрессии: службы помощи личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).

2. Требования к знаниям и умениям:

Обучающиеся должны знать сетевой этикет, этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность.

Обучающиеся должны уметь использовать этические и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность.

3. Тематика практических работ:

Практическая работа «Выпуск видеоролика на тему «Как не испортить себе настроение при общении в Сети и не опуститься до уровня «веб-агрессора".

Тема №7 Государственная политика в области кибербезопасности.

1. **Основные вопросы:** Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация. Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера. Как расследуются преступления в сети. Ответственность за интернет – мошенничество. Правовые акты в области информационных технологий и защиты киберпространства. Доктрина информационной безопасности.

2. **Требования к знаниям и умениям:**

Обучающиеся должны знать правовые основы защиты от информации, причиняющей вред здоровью и развитию, интеллектуальной собственности, уголовной ответственности за создание, использование и распространение вредоностных компьютерных программ, авторского право, охраны программ для ЭВМ и баз данных (БД), лицензионных программ.

Обучающиеся должны уметь пользоваться правовыми основами защиты от информации, причиняющей вред здоровью и развитию, интеллектуальной собственности, уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ, авторским правом, охраны программ для ЭВМ и баз данных(БД), лицензионных программ.

3. **Тематика практических работ:**

Практическая работа №1 «Буклет Правовые основы для защиты от спама»

Практическая работа №2 «Создание презентации «Как уберечь свою персональную информацию в Интернете, если вы общаетесь в социальных сетях».

III. Тематическое планирование с указанием количества часов, отводимых на освоения каждой темы.

№ п/п	Тема	Всего часов	Теоретические занятия	Практические занятия
1.	Общие сведения о безопасности ПК и Интернете.	5	4	1
2.	Техника безопасности и экология.	5	4	1
3.	Проблемы Интернет – зависимости.	5	4	1
4.	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	5	4	1
5.	Мошеннические действия в Интернете. Киберпреступления.	5	4	1
6.	Сетевой этикет. Психология и сеть.	5	4	1
7.	Государственная политика в области кибербезопасности.	4	3	1
	Итого	**34**	**27**	**7**

Тематическое планирование
по внеурочной деятельности «Безопасный Интернет»
для 8 класса (34 часа, 1 ч. в неделю)

№	Тема	Кол.-во часов	Дата		Примечание
			По плану	Фактич.	
Общие сведения о безопасности ПК и Интернета (5 часов)					
1.	Как устроены компьютер и Интернет.	1			
2.	Как работают мобильные устройства. Угрозы для мобильных устройств.	1			
3.	Защита персональных данных.	1			
4.	Компьютерная и информационная безопасность. Основные угрозы безопасности информации.	1			
5.	ПР №1 «Создание газеты «Безопасность в Интернете»	1			
Техника безопасности и экология (5 часов)					
6.	Правила поведения в компьютерном кабинете.	1			
7.	Компьютер и мобильные устройства в чрезвычайных ситуациях.	1			
8.	Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду	1			
9.	Комплекс упражнений при работе за компьютером. Гигиена при работе с ПК.	1			
10.	ПР №2 «Создание буклета «Техника безопасности при работе с компьютером»	1			

Проблемы Интернет – зависимости (5 часов)					
11.	ЗОЖ и компьютер. Деструктивная информация в Интернете как ее избежать.	1			
12.	Психологическое воздействие информации на человека. Управление личностью через сеть.	1			
13.	Интернет и компьютер зависимость (аддикция).	1			
14.	Как развивается зависимость. Типы интернет – зависимости.	1			
15.	ПР №3 «Создание мультимедийной презентации «ПК и ЗОЖ. Организация рабочего места».	1			
Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (5 часов)					
16.	Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов.	1			
17.	Отличия вирусов и закладок. Как распространяются вирусы. ПР №4 «Создание презентации на тему «Разновидности вирусов. Черви трояны, скрипты».	1			
18.	Что такое антивирусная защита. Как лечить компьютер.	1			
19.	Антивирусные программы для ПК. Выявление неизвестных вирусов. ПР №5 «Установка антивирусной программы».	1			
20.	Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.	1			
Мошеннические действия в Интернете. Киберпреступления (5 часов)					
21.	Виды интернет – мошенничества. Мошеннические действия в сети.	1			
22.	Предложения о разблокировании программ. Ложные антивирусы.	1			
23.	«Легкий заработок в Интернете». Мошенничество при распространении «бесплатного» ПО. Азартные игры. Онлайн – казино.	1			
24.	Технологии манипулирования в Интернете. Техника	1			

	безопасности при интернет – общении.				
25.	ПР №6 «Доклад на тему: «Правила поведения в сети с мошенниками и злоумышленниками».	1			
Сетевой этикет. Психология и сеть (5 часов)					
26.	Что такое этикет. Виды этикета.	1			
27.	Сетевой этикет. Общие правила сетевого этикета. Этикет и безопасность.	1			
28.	Безопасная работа в сети в процессе сетевой коммуникации.	1			
29.	Психологическая обстановка в Интернете. Если вы стали жертвой компьютерной. Агрессии.	1			
30.	ПР №7 «Выпуск видеоролика на тему « Как не испортить себе настроение при общении в Сетии не опуститься до уровня «веб – агрессора».	1			
Государственная политика в области кибербезопасности (4 часа)					
31.	Собственность в Интернете. Авторское право. Интеллектуальная собственность.	1			
32.	Платная и бесплатная информация. Защита прав потребителей при использовании услуг Интернет.	1			
33.	Как расследуются преступления в сети. Ответственность за интернет – мошенничество.	1			
34.	Правовые акты в области информационных технологий и защиты киберпространства.	1			