

Муниципальное бюджетное общеобразовательное учреждение
Петрозаводского городского округа
«Средняя общеобразовательная школа № 46»

«Утверждаю»

Директор школы

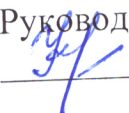
Петрова Ж.Л.

«10» августа 2020 г.

Приказ № 3

Рабочая программа учебного предмета «Информационная безопасность»

Основное общее образование
(срок освоения 1 год)

Согласована
на заседании методического объединения
Протокол № 4
от «06» мая 2020 года
Руководитель МО
 (Г.Н.Фурса)

Принята
на педагогическом совете
Протокол № 1
от «30» августа 2021 года

Петрозаводск
2021 г.

Раздел 1. Планируемые результаты освоения учебного предмета

Курс ориентирован на проведение уроков по информационной безопасности школьников и безопасному поведению в сети Интернет. Он отражает актуальные вопросы безопасной работы с персональной информацией, сообщениями и звонками по мобильному телефону, электронной почтой, информационными и коммуникационными ресурсами в сети Интернет, доступа к ресурсам для досуга, поиска новостной, познавательной, учебной информации, общения в социальных сетях, получения и передачи файлов, размещения личной информации в коллективных социальных сервисах.

Цель программы: создание условий для формирования у обучающихся знаний, умений и навыков, необходимых для организации безопасного поведения в сети Интернет и безопасности личного информационного пространства.

Задачи программы:

- дать представление о современном информационном обществе, информационной безопасности личности и государства;
- сформировать навыки ответственного и безопасного поведения в современной информационно-телекоммуникационной среде;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом;
- сформировать общекультурные навыки работы с информацией (умений грамотно пользоваться источниками информации, правильно организовать информационный процесс);
- дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;
- познакомить со способами защиты от противоправных посягательств в сети Интернет, защиты личных данных.

Предметные результаты:

- умение 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;
- формирование представлений о существующих киберугрозах и правилах действий при встрече с ними в глобальной сети;
- умение защитить себя и технические устройства при обнаружении ошибок и заражения вредоносными программами;
- понимание основ правовых аспектов использования компьютерных программ и работы в Интернете;

Метапредметные результаты:

- умение самостоятельно определять цели и задачи деятельности, составлять планы, контролировать и корректировать их выполнение;
- умение продуктивно общаться и взаимодействовать в процессе совместной деятельности;
- владение навыками познавательной, учебно-исследовательской и проектной деятельности, способность и готовность к самостоятельному поиску методов решения практических задач;
- умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию;

Личностные результаты:

- 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 ценности безопасного образа жизни;
- интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Раздел 2. Содержание учебного предмета

Основное содержание программы представлено 4 разделами «Информация», «Киберпространство», «Киберкультура», «Киберугрозы».

Учебный курс позволяет создать условия для формирования активной позиции школьников в получении знаний и умений, выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы, противостоять им. Производится профилактика негативных тенденций в развитии информационной культуры учащихся для повышения защищенности детей от информационных рисков и угроз.

Система заданий предполагает индивидуальную и групповую формы работы, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах. Предлагаемые задания направлены на формирование критичного мышления школьников, формирование умений решать проблемы, работать в команде, высказывать и защищать собственную позицию, приобретение основ безопасной работы с информацией в виртуальном мире.

Раздел 3. Тематическое планирование

№	Тема	Основное содержание
Раздел 1 «Информация»		
1.	Информация. Виды информации.	Понятие «Информация». Действия с информацией. Виды информации по назначению. Характеристики информации.
2.	Информационная безопасность. Цель и задачи информационной безопасности.	Понятие «Информационная безопасность». Цель, задачи информационной безопасности.
3.	Виды угроз информационной безопасности.	Виды угроз информационной безопасности: техногенные источники, антропогенные источники, стихийные источники
4.	Практическая работа №1 «Виды угроз информационной безопасности»	Работа в группах «Виды угроз информационной безопасности»
5.	Нормативно-правовые основы информационной безопасности в РФ.	Основные документы в области информационной безопасности Российской Федерации. Информация как объект правовых отношений. Виды юридической ответственности.
6.	Обсуждение "Информация. Информационная безопасность"	Актуализация знаний
Раздел 2 «Киберпространство»		
7.	Урок Цифры «Искусственный интеллект в образовании»	Создание умного помощника для учителя. Помощь искусственного интеллекта в работе человека.
8.	Киберпространство	Понятие «Киберпространство». Составляющие киберпространства. Сервисы глобальной сети. Понятие «Кибербезопасность».
9.	Кибермиры	Понятие «Кибермиры». Смарт-технологии. Искусственный интеллект. Экзоскелет.
10.	Киберфизическая система	Понятие «Киберфизическая система». Умная система. Ключевые технологии, используемые в киберфизических системах.
11.	Киберобщество	Понятие «Киберобщество». Особенность киберобщества. Информационный мир. Сетевой этикет. Клиповое мышление. Кибермания. Киберграждане.
12.	Киберденьги	Понятие «Киберденьги». Электронные деньги. Управление электронными деньгами. Кибермошейничество. Виды кибермошейничества.
13.	Обсуждение и тест по теме «Киберпространство»	Актуализация знаний.
14.	Практическая работа №2 «Безопасные онлайн-платежи»	Закрепление изученного материала
Раздел 3 «Киберкультура»		
15.	Киберкультура	Понятие «Киберкультура». Киберискусство. Виды компьютерного искусства.
16.	Знакомство с интернет-ресурсами о культуре	Онлайн-ресурсы.

17.	Электронные книги. Киберкниги.	Электронная книга. Авторское право. AR-книги. Виртуальная реальность.
18.	Киберискусство	Понятие «Киберискусство». Виды киберискусства.
19.	Урок Цифры «Исследование кибератак»	Обнаружение кибератаки и её исследование. Распознавание фишинговых сайтов, создание надежных паролей.
20.	Социальная инженерия	Понятие «Социальная инженерия». Техники социальной инженерии в Интернете.
21.	Классификация угроз социальной инженерии	Угрозы, исходящие от использования телефоном. Угрозы, исходящие от электронных писем (фишинг). Угрозы при использовании мессенджеров. Кража личности
22.	Практическая работа №3 «Безопасный интернет»	Закрепление изученного материала
23.	Урок Цифры «Приватность в цифровом мире»	Овладение навыком защиты свои персональных данных.
Раздел 4 «Киберугрозы»		
24.	Киберугрозы. Кибервойны	Понятия «Киберугроза», «Кибервойна». Виды кибервойн. Цель, задачи, оружие, инструмент кибервойны. Виды оружия в кибервойне. Виды кибератак.
25.	Киберприступность	Виртуальные правонарушения. Преступления, совершаемые в Интернете. Понятие «Киберприступность». Группы киберприступности. Объекты киберприступности. Мотивы правонарушителей.
26.	Киберпреступления	Киберсталкинг. Кибертерроризм. Тайпсквоттинг. Глава 8 уголовного кодекса РФ
27.	Уязвимости кибербезопасности	Понятие «Кибербезопасность». Цель Кибербезопасности. Уязвимость. Методы атак.
28.	Угрозы информационной безопасности	Понятие «Угрозы ИБ». Типы угроз. Преднамеренные и непреднамеренные угрозы. Группы угроз ИБ.
29.	Запрещённые и нежелательные сайты	Единый реестр сетевых адресов, указателей интернет-страниц и доменных имен. Веб-фильтры. Роскомнадзор.
30.	Резервное копирование данных	Безопасность личной информации. Создание резервных копий на различных устройствах.
31.	Новые профессии в киберобществе	Атлас профессий. Требования к новым профессиям
32.	Практическая работа №5	«Безопасность в интернете»
33.	Викторина «Информационная безопасность»	Актуализация знаний курса «Информационная безопасность»
34.	Подведение итогов курса «Информационная безопасность»	Высказывание личного мнения. Обсуждение.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 603332450510203670830559428146817986133868575789

Владелец Кормакова Анастасия Викторовна

Действителен с 29.03.2022 по 29.03.2023