Муниципальное общеобразовательное автономное учреждение
средняя общеобразовательная школа № 3
городского округа город Нефтекамск Республики Башкортостан

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
Руководитель ШМО	Заместитель директора по ВР	Директор МОАУ СОШ № 3
Шарафиева Г.Ф.	Леготина С.В.	Крылов А.В.
Протокол № 1 от 28.08.2023 г.	Протокол № 01 от 30.08.2023 г.	Приказ № 419 от 31.08.2023 г.

МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 3 ГОРОДСКОГО ОКРУГА ГОРОД НЕФТЕКАМСК РЕСПУБЛИКИ БАШКОРТОСТАН

Подписан: МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 3 ГОРОДСКОГО ОКРУГА ГОРОД НЕФТЕКАМСК РЕСПУБЛИКИ БАШКОРТОСТАН
DN: C=RU, S=Республика Башкортостан, STREET="пр.Комсомольский д.17 ""Б""", L=г. Нефтекамск, T=Исполняющий обязанности директора, O=МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 3 ГОРОДСКОГО ОКРУГА ГОРОД НЕФТЕКАМСК РЕСПУБЛИКИ БАШКОРТОСТАН, ОГРН=1020201882623, СНИЛС=02256414319, ИНН ЮЛ=0264012552, ИНН=026408749174, E=nur.aigul78@mail.ru, G=Марина Михайловна, SN=Сакратова, CN=МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 3 ГОРОДСКОГО ОКРУГА ГОРОД НЕФТЕКАМСК РЕСПУБЛИКИ БАШКОРТОСТАН
Основание: Я являюсь автором этого документа
Местоположение:
Дата: 2023-11-10 09:14:29

РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

«Информационная безопасность»

6 класс

Курс «Информационная безопасность»

Уровень образования: основное общее образование

Количество часов по программе: 34 часов

Автор-составитель: Микитанова А.Ю.

Нефтекамск 2023

Содержание программы:

Пояснительная записка

Рабочая программа по внеурочной деятельности для 6 классов составлена на основе следующих нормативных документов:

Закон Российской Федерации от 29.12.2012г. №273-ФЗ «Об образовании в Российской Федерации»;

Приказ Министерства образования и науки Российской Федерации 17.12.2010 № 1897

«Об утверждении федерального государственного образовательного стандарта основного общего образования»;

Приказ МО и Н РФ от 17 декабря 2010 г. N 1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования» (в ред. Приказов Минобрнауки России от 29.12.2014 N 1644, от 31.12.2015 N 1577) Зарегистрировано в Минюсте России 1 февраля 2011 г. N 19644

Приказы МО и Н РФ от 31 декабря 2015 года № 1577 «О внесении изменений в ФГОС ООО, утвержденный приказом МОиН РФ от 17 декабря 2010 г. № 1897» (зарегистрирован Минюстом России 2 февраля 2016 г., регистрационный № 40937).

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.

Цель программы:

Обеспечить условия для профилактики негативных тенденций в информационной культуре учащихся, повышение защищённости детей от информационных рисков и угроз, формирование навыков распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Планируемые результаты освоения курса внеурочной деятельности

Личностные результаты

- умение грамотно излагать свои мысли в устной и письменной речи;
- критичность мышления, умение распознавать достоверную информацию;
- представление об информатике как сфере человеческой деятельности, о её значимости для развития цивилизации;
- активность при решении практических задач по основам информационной безопасности;
- умение контролировать процесс и результат учебной деятельности.

Метапредметные результаты:

- самостоятельно анализировать условия достижения цели на основе учета выделенных ориентиров действия в новом учебном материале;
- планировать пути достижения целей;
- уметь самостоятельно контролировать свое время и управлять им;
- сравнивать разные точки зрения, прежде чем принимать решения и выполнять практические действия;
- аргументировать свою точку зрения, спорить и отстаивать свою позицию невраждебным для оппонентов образом;
- задавать вопросы, необходимые для организации собственной деятельности и сотрудничества с партнером;
- осуществлять взаимный контроль и оказывать в сотрудничестве необходимую взаимопомощь;
- применять современные информационные технологии для коллективной, групповой и индивидуальной работы;
- осуществлять расширенный поиск информации с использованием ресурсов Интернета;

- владеть навыками ознакомительного, изучающего, усваивающего и поискового чтения;
- осуществлять выбор наиболее эффективных способов решения практических задач в сфере личной информационной безопасности в зависимости от конкретных условий;
- владеть навыками безопасного и целесообразного поведения при работе в информационном пространстве, соблюдать нормы информационной этики и права.

Предметные результаты:

- знать основные термины и понятия по проблематике информационной безопасности;
- знать основные положения нормативных документов в РФ, регламентирующих стратегию развития информационного общества России, защиту информации и баз данных, административную и уголовная ответственность в сфере информационной безопасности;
- знать разновидности угроз информационной безопасности государству и личности;
- знать принципы и методы организационной защиты информации;
- уметь выявлять и уничтожать компьютерные вирусы;
- уметь использовать методы защиты личного информационного пространства.

Ожидаемые результаты обучения

После прохождения курса учащиеся должны знать:

- понятие и угрозы информационной безопасности,
- уровни защиты информации,

- меры защиты информации,
- правовые акты и нормы по защите информации и авторского права,
- программно-технические меры по защите информации,
- принципы и приемы сетевой безопасности

уметь:

- использовать возможности ОС WindowsXP для защиты информации;
- применять на практике меры профилактики и защиты информации.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

6 КЛАСС

Раздел 1. Информационная безопасность (34 час)

Тема 1. Безопасность общения (16 часов)

Общение в социальных сетях и мессенджерах. Создание безопасных паролей. Настройки социальных сетей. Безопасное размещение материалов в социальных сетях. Травля в социальных сетях. Ложные сайты и письма.

Тема 2. Безопасность устройств (8 часов)

Вредоносные программы. Способы борьбы с компьютерными вирусами.

Тема 3. Безопасность информации (8 часов)

Манипулирование людьми в социальных сетях, глобальных сетях и СМИ. Ложная информация. Проведение безопасных расчётов в Интернете. Безопасность при использовании беспроводных сетей. Сохранение цифровых данных.

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ
6 КЛАСС

№ п/п	Тема урока	Количество часов		
		Всего	Теория	Практические работы
Раздел 1. Информационная безопасность (34 часа)				
Тема 1. Безопасность общения (16 часов)				
1	Общение в социальных сетях и мессенджерах	1	1	
2	С кем безопасно общаться в интернете	1	1	
3	Выбор безопасного собеседника в социальной сети	1		1
4	Пароли для аккаунтов в социальных сетях	1	1	
5	Составление безопасных паролей	1		1
6	Вход в аккаунт социальных сетей	1	1	
7	Игра-соревнование «Безопасное поведение в социальных сетях»	1		1
8	Настройки конфиденциальности в социальных сетях и мессенджерах	1	1	
9	Как настроить конфенденциальность в социальной сети	1		1
10	Публикация информации в социальных сетях	1	1	
11	Выбор личной информации для безопасного, нейтрального и опасного размещения.	1		1
12	Кибербуллинг	1	1	
13	Как не стать жертвой	1		1

	кибербуллинга			
14	Фишинг	1	1	
15	Определение признаков фишинга в адресах и письмах	1		1
16	Защита проекта «Социальные сети»	1		1
Тема 2. Безопасность устройств (8 часов)				
17	Что такое вредоносный код	1	1	
18	Распространение вредоносного кода	1	1	
19	Определение объектов, могущих содержать вредоносный код	1		1
20	Методы защиты от вредоносных программ	1	1	
21	Разработка мероприятий по защите компьютера от вредоносных программ	1		1
22	Антивирусная программа	1		1
23	Вредоносный код и мобильные устройства	1	1	
24	Представление стенгазеты «Компьютерный вирус»	1		1
Тема 2. Безопасность информации (10 часов)				
25	Социальная инженерия	1	1	
26	Нахождение признаков применения социальной инженерии	1		1
27	Ложная информация в Интернете	1	1	
28	Подтверждение или опровержение информации	1		1
29	Безопасность платежей в Интернете	1	1	
30	Разработка памятки проведения безопасных платежей	1		1
31	Беспроводная связь	1	1	

32	Резервное копирование данных	1	1	
33	Разработка теста «Грозит ли вам опасность в интернете?»	1		1
34	Анализ данных по тестированию	1		1
	ИТОГО по разделу	**34**	**17**	**17**
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		**34**		