

Государственное бюджетное общеобразовательное учреждение Самарской области  
средняя общеобразовательная школа с.Узюково  
муниципального района Ставропольский Самарской области

«ПРИНЯТО»  
на Педагогическом совете  
Учреждения  
протокол № 12 от  
« 29 » 08 20 19 г.



**РАБОЧАЯ ПРОГРАММА**  
по внеурочной деятельности «Информационная безопасность, или  
на расстоянии одного вируса»

Направление: общеинтеллектуальное  
Класс: 8  
Программа утверждена на 1 год.  
Составитель: Кондакова И.М.

2019 год

## Содержание

1. Пояснительная записка
2. Планируемые результаты изучения учебного предмета
3. Содержание внеурочной деятельности
4. Тематическое планирование

### 1. Пояснительная записка

Рабочая программа по внеурочной деятельности составлена на основе:

- Федерального закона «Об образовании в Российской Федерации» № 273-ФЗ от 29 декабря 2012 г.
- Федерального государственного образовательного стандарта основного общего образования (приказ МОиН РФ № 1644 от 29.12.2014г.)
- Примерной основной образовательной программы основного общего образования, одобренной федеральным учебно-методическим объединением по общему образованию(протокол от 8.04.2015г №1/15)
- Основной образовательной программы основного общего образования ГБОУ СОШ с.Узюково
- Положения о рабочей программе по внеурочной деятельности ГБОУ СОШ с.Узюково
- Федерального закона «Об информатизации, информационных технологиях и о защите информации» от 27 июля 2006 года.
- Учебного пособия М.С. Наместниковой «Информационная безопасность, или на расстоянии одного вируса»- М.: Просвещение. 2015.

Внеурочная деятельность «Информационная безопасность, или на расстоянии одного вируса» *предназначена* для внеурочной работы и рассчитана на учащихся 8-х классов, интересующихся информатикой. В данной программе рассмотрены основные разделы дисциплины «Информационная безопасность и защита информации», содержащие описание объекта защиты, классификацию угроз и методов защиты информации. Значительное место уделено методам формирования целостного представления об информационной безопасности, угрозах информационной безопасности и защите информации, формированию знаний, умений и навыков о защите информации, представленной в электронном виде, изучению современных технологии борьбы с вредоносными программами.

*Курс рассчитан* на 34 часа.

### **Задачи:**

- **обучающие:** сформировать целостное представление об информационной безопасности, опасности в глобальной сети для подростков, умение использовать полученные знания на практике, в условиях решения реальных задач

-**развивающие:** развитие навыка логического, аналитического мышления, развитие навыков критического мышления, создание условий для развития познавательных потребностей учащихся.

-**воспитательные:** показать возможность применения теоретических знаний при решении повседневных задач, показать связь информатики с жизнью.

### **Цели :**

#### **Познавательные:**

- Находить (в источниках) достоверную информацию, необходимую для решения учебных и жизненных задач.
- Владеть смысловым чтением – самостоятельно вычитывать концептуальную информацию, необходимую для решения поставленной задачи.
- Сравнивать объекты по заданным или самостоятельно определенным критериям.
- Представлять информацию в компактном виде (таблицы, памятки)

#### **Регулятивные:**

- Определять цель, проблему в деятельности: учебной и жизненно-практической (в т.ч. в своём задании).
- Выдвигать версии, выбирать средства достижения цели в группе и индивидуально.
- Работать по плану, сверяясь с целью, находить и исправлять ошибки.

#### **Коммуникативные:**

- Излагать свое мнение (в монологе, диалоге), аргументируя его, подтверждая фактами, выдвигая контраргументы в дискуссии.
- Различать в речи другого мнения, доказательства, факты; гипотезы, аксиомы, догматы, теории.
- Организовывать работу в паре (самостоятельно определять цели, роли, задавать вопросы, вырабатывать решения).
- Использовать ИКТ как инструмент для достижения своих целей.

#### **Личностные:**

вырабатывать уважительно-доброжелательное отношение к людям, идти на взаимные уступки в разных ситуациях.

## **2. Планируемые результаты изучения учебного предмета**

В результате освоения учебной дисциплины обучающийся должен **иметь практический опыт:**

- использования информационных и коммуникационных технологий на различных этапах профессиональной деятельности;
- использование ресурсов сети Интернет для поиска информации;

- работа с базами данных, электронными библиотеками, компьютерными справочными системами.

В результате освоения учебной дисциплины обучающийся должен **уметь:**

- работать с электронными документами;
- применять мультимедийные технологии;
- вести прием и передачу сообщений по электронной почте;
- обеспечивать надежное хранение документов и данных.

В результате освоения учебной дисциплины обучающийся должен **знать:**

- безопасность работы в сети Интернет;
- состав, функции и возможности телекоммуникативных технологий;
- виды и правила сетевого взаимодействия.

### **3.Содержание внеурочной деятельности**

#### **Безопасность общения(17 ч)**

Общение в социальных сетях и мессенджерах. С кем безопасно общаться в Интернете

Пароли для аккаунтов в социальных сетях. Как выполнять Вход в аккаунт.Как настроить конфиденциальность в социальных сетях. Что и как публиковать в социальных сетях.

Что такое кибербуллинг и как с ним работать.Как работать в публичных аккаунтах.

Что такое Фишинг.

#### **Безопасность устройств(4 ч)**

Понятие Вредоносного кода,как его различить и узнать.

Распространение вредоносного кода(как это происходит). Методы защиты от вредоносных программ

Распространение вредоносного кода на мобильных устройствах

#### **Безопасность информации(13 ч)**

Понятие «Социальная инженерия»,область применения. Ложная информация в Интернете

Безопасность при использовании платежных карт(как защитить от взлома)

Понятие «Беспроводная технология связи» и « Безопасность общения»

Резервное копирование данных(методы и принципы)

Безопасность устройств(антивирусные программы и методы их использования)

Безопасность информации(как защищать информацию)

#### 4. Тематическое планирование

Перечень разделов и тем	Кол-во часов	Аудиторные	Внеаудиторные
<b>Тема 1. Безопасность общения</b>	<b>17</b>		
Общение в социальных сетях и мессенджерах	2	2	
С кем безопасно общаться в Интернете	2		2
Пароли для аккаунтов в соц.сетях	2		2
Вход в аккаунт	1	1	
Настройки конфиденциальности в соц.сетях	1	1	
Публикация информации в соц.сетях	3	3	
Кибербуллинг	2	2	
Публичные аккаунты	2	2	
Фишинг	2	2	
<b>Тема 2.Безопасность устройств</b>	<b>4</b>		
Вредоносный код.	1		1
Распространение вредоносного кода.	1	1	
Методы защиты от вредоносных программ	1		1
Распространение вредоносного кода на мобильных устройствах	1		1
<b>Тема 3. Безопасность информации</b>	<b>13</b>		
Социальная инженерия	1		1
Ложная информация в Интернете	1	1	
Безопасность при использовании платежных карт	1	1	
Беспроводная технология связи	1	1	
Резервное копирование данных	1	1	
Безопасность общения	1	1	
Безопасность устройств	1		1
Безопасность информации	1	1	
Работа над проектами.	3		3
Защита проектов.	1	1	
Защита проектов. Заключительное занятие.	1	1	
<b>Итого</b>	<b>34</b>	<b>22</b>	<b>12</b>