

**Северное управление министерства образования и науки  
самарской области  
государственное бюджетное общеобразовательное учреждение самарской области  
средняя общеобразовательная школа с. Калиновка муниципального района  
Сергиевский  
Самарской области**

РАССМОТРЕНО и  
РЕКОМЕНДОВАНА  
на заседании ШМО учителей  
естественно-научного  
и- математического цикла  
№ протокола 1  
от «\_\_\_» \_\_\_\_\_ 20\_\_ г.  
Руководитель К.И.Щетинина

ПРОВЕРЕНО  
заместитель директора  
по УВР  
Е.В. Шишкина  
\_\_\_\_\_  
«\_\_\_» \_\_\_\_\_ 20\_\_ г.

УТВЕРЖДАЮ  
Директор ГБОУ СОШ  
с. Калиновка  
С.В. Субаев  
\_\_\_\_\_  
от «\_\_\_» \_\_\_\_\_ 20\_\_ г.

**РАБОЧАЯ ПРОГРАММА**  
**внеурочной деятельности «Информационная безопасность»**  
**на уровне основного общего**  
**образования**  
(наименование курса, направленность, уровень обучения)  
**9 класс, 34 часа.**  
(классы освоения, количество часов)

Рабочая программа ГБОУ СОШ с. Калиновка курса внеурочной деятельности «Информационная безопасность» на уровне основного общего образования (9 класс) составлена с учетом требований Федерального государственного образовательного стандарта основного общего образования (утвержден приказом министерства образования и науки Российской Федерации № 1897 от 17.12.2010 в редакции приказов Минобрнауки № 1644 от 29.12.2014 и № 1577 от 31.12.2015), в соответствии с основной образовательной программой основного общего образования ГБОУ СОШ с. Калиновка и является модифицированной общеобразовательной программой, составленной на основе примерной рабочей программы учебного курса «Цифровая гигиена», основного общего образования. Рекомендовано координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол №27 от 21.08.2019), Самара. Составлена на основе программы:

<b>Класс</b>	<b>Предмет</b>	<b>Программа</b>
7	Информационная безопасность, или на расстоянии одного вируса	Примерная рабочая программа учебного курса «Цифровая гигиена». 7-9 классы. – Самара.

В Учебном плане ГБОУ СОШ с. Калиновка на изучение курса внеурочной деятельности «Информационная безопасность» отводится в 9 классе – 1 час в неделю, что составляет 34 часа в год.

Итого на уровне основного общего образования на внеурочную деятельность отводится – 34 часа.

### **1. Планируемые результаты освоения курса внеурочной деятельности «Информационная безопасность, или на расстоянии одного вируса»**

Личностные результаты отражаются в индивидуальных качественных свойствах учащихся, которые они должны приобрести в процессе освоения курса. К личностным результатам относят:

- 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.

Метапредметные результаты характеризуют уровень сформированности универсальных способностей учащихся, проявляющихся в познавательной и практической творческой деятельности, таких как:

- ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- 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;
- 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.

Достижение предметных результатов образовательной программы общественно-научных предметов даст учащимся возможность:

Выпускник 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.

Выпускник овладеет:

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

Выпускник получит возможность овладеть:

- основами соблюдения норм информационной этики и права;
- основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;
- использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет ресурсы и другие базы данных.

## **2. Содержание курса внеурочной деятельности с указанием форм организации и видов деятельности**

### **«Информационная безопасность, или на расстоянии одного вируса»**

#### **Раздел 1. «Безопасность общения»**

##### **Тема 1. Общение в социальных сетях и мессенджерах.**

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент. **Тема 2.**

##### **С кем безопасно общаться в интернете.**

Персональные данные как основной капитал личного пространства в цифровом мире.

Правила добавления друзей в социальных сетях. Профиль пользователя.

Анонимные социальные сети. **Тема 3. Пароли для**

##### **аккаунтов социальных сетей.**

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей. **Тема 4. Безопасный вход в аккаунты.**

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

##### **Тема 5. Настройки конфиденциальности в социальных сетях.**

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

## **Тема 6. Публикация информации в социальных сетях.**

Персональные данные. Публикация личной информации.

## **Тема 7. Кибербуллинг.**

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать?

Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. **Тема**

## **8. Публичные аккаунты.**

Настройки приватности публичных страниц. Правила ведения публичных страниц.

## **Тема 9. Фишинг.**

Фишинг как мошеннический прием. Популярные варианты распространения фишинга.

Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

## **Выполнение и защита индивидуальных и групповых проектов .**

### **Раздел 2. «Безопасность устройств»**

#### **Тема 1. Что такое вредоносный код.**

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

#### **Тема 2. Распространение вредоносного кода.**

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах. **Тема 3. Методы защиты от вредоносных программ.**

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов. **Тема 4.**

#### **Распространение вредоносного кода для мобильных устройств.**

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

## **Выполнение и защита индивидуальных и групповых проектов.**

### **Раздел 3 «Безопасность информации»**

#### **Тема 1. Социальная инженерия: распознать и избежать.**

Приемы социальной инженерии. Правила безопасности при виртуальных контактах. **Тема**

#### **2. Ложная информация в Интернете.**

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

#### **Тема 3. Безопасность при использовании платежных карт в Интернете.**

Транзакции и связанные с ними риски. Правила совершения онлайн покупок.

Безопасность банковских сервисов.

#### **Тема 4. Беспроводная технология связи.**

#### **Тема 5. Резервное копирование данных.**

Безопасность личной информации. Создание резервных копий на различных устройствах.

#### **Тема 6. Основы государственной политики в области формирования культуры информационной безопасности.**

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

**Выполнение и защита индивидуальных и групповых проектов. Повторение. Волонтерская практика.**

**3. Тематическое планирование с указанием количества часов на освоение каждой темы.**

№	Тема ( раздел)	количество часов на изучение	Используемое оборудование центра «Точка роста»
<b>«Информационная безопасность, или на расстоянии одного вируса» 7 класс (1 час в неделю, всего 34 часа)</b>			
1	Общение в социальных сетях и мессенджерах	1	Образовательный набор для изучения
2	С кем безопасно общаться в интернете	1	многокомпонентных робототехнических систем и манипуляционных роботов
3	Пароли для аккаунтов социальных сетей	1	
4	Безопасный вход в аккаунты	1	
5	Настройки конфиденциальности в социальных сетях	1	
6	Публикация информации в социальных сетях	1	
7	Кибербуллинг	1	Образовательный набор для изучения
8	Публичные аккаунты	1	многокомпонентных робототехнических систем и
9-10	Фишинг	2	
11-13	Выполнение и защита индивидуальных и групповых проектов	3	манипуляционных роботов
14	Что такое вредоносный код	1	
15	Распространение вредоносного кода	1	

16-17	Методы защиты от вредоносных программ	2	
18	Распространение вредоносного кода для мобильных устройств	1	
19-21	Выполнение и защита индивидуальных и групповых проектов	3	
22	Социальная инженерия: распознать и избежать	1	
23	Ложная информация в Интернете	1	Образовательный набор для изучения многокомпонентных робототехнических систем и манипуляционных роботов
24	Безопасность при использовании платежных карт в Интернете	1	
25	Беспроводная технология связи	1	
26	Резервное копирование данных	1	
27-28	Основы государственной политики в области формирования культуры информационной безопасности	2	
29-31	Выполнение и защита индивидуальных и групповых проектов	3	
32-34	Повторение, волонтерская практика, резерв	3	