

**Государственное бюджетное общеобразовательное учреждение  
Самарской области основная общеобразовательная школа №9  
имени Героя Советского Союза И.Д.Ваничкина  
города Новокуйбышевска городского округа Новокуйбышевск  
Самарской области**

446218, Самарская область, г. Новокуйбышевск, ул. Ворошилова, д. 6, тел. 4-70-52

**Принято  
на заседании  
Педагогического совета  
Протокол № 1  
от «29» августа 2022 г.**

**Утверждено  
приказом директора № 326-од  
от 29.08.2022 г.  
Директор ГБОУ ООШ № 9  
\_\_\_\_\_ Г.Н. Недбало**

***Рабочая программа внеурочной деятельности***

***«Информационная безопасность»***

***7 классы***

**Составитель:  
*Невзорова О.Н., учитель математики***

**2022**

## **Введение**

Рабочая программа внеурочной деятельности учебного курса «Информационная безопасность» (далее – Программа) предназначена для обучающихся 7 классов и рассчитана на 1 год обучения.

Программа включает три раздела:

- «Планируемые результаты освоения курса внеурочной деятельности»;
- «Содержание курса внеурочной деятельности»;
- «Тематическое планирование».

Программа разработана в соответствии с:

- Примерной рабочей программой учебного курса «Цифровая гигиена», рекомендованной Координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019)

- Основной образовательной программой основного общего образования ГБОУ ООШ № 9 г. Новокуйбышевска.

## **Планируемые результаты освоения курса внеурочной деятельности**

### **Личностные**

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

### **Метапредметные**

Регулятивные универсальные учебные действия:

- идентифицировать собственные проблемы и определять главную проблему;
- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- составлять план решения проблемы (выполнения проекта, проведения исследования);
- описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия:

- выделять явление из общего ряда других явлений;

- 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;
- излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- критически оценивать содержание и форму текста;
- определять необходимые ключевые поисковые слова и запросы.

**Коммуникативные универсальные учебные действия:**

- строить позитивные отношения в процессе учебной и познавательной деятельности;
- 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;
- выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
- использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
- использовать информацию с учетом этических и правовых норм;
- создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

**Предметные:**

- 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.
- владеть приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.
- владеть основами соблюдения норм информационной этики и права;
- владеть 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.

## **Содержание курса внеурочной деятельности**

Содержание программы учебного курса соответствует темам основной образовательной программы основного общего образования по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Учебный курс «Информационная безопасность» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей.

Основными **целями** изучения учебного курса «Информационная безопасность» являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
- формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

**Задачи** программы:

- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
- создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
- сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
- сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;

- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

За счет часов, предусмотренных для повторения материала (4 часа), возможно проведение занятий для учащихся 4-6 классов. Эти занятия в качестве волонтерской практики могут быть проведены учащимися, освоившими программу. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные в ходе выполнения учебных заданий по основным темам курса.

## **7 класс (34 ч.)**

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

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

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

#### **Тема 2. С кем безопасно общаться в интернете. 1 час.**

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. 1 час.**

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

#### **Тема 4. Безопасный вход в аккаунты. 1 час.**

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

#### **Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.**

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

#### **Тема 6. Публикация информации в социальных сетях. 1 час.**

Персональные данные. Публикация личной информации.

#### **Тема 7. Кибербуллинг. 1 час.**

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

#### **Тема 8. Публичные аккаунты. 1 час.**

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

#### **Тема 9. Фишинг. 2 часа.**

Фишинг как мошеннический прием. Популярны варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

**Выполнение и защита индивидуальных и групповых проектов. 3 часа.**

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

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

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

**Тема 2. Распространение вредоносного кода. 1 час.**

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. 2 часа.**

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

**Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.**

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

**Выполнение и защита индивидуальных и групповых проектов. 3 часа.**

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

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

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

**Тема 2. Ложная информация в Интернете. 1 час.**

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

**Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.**

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

**Тема 4. Беспроводная технология связи. 1 час.**

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

**Тема 5. Резервное копирование данных. 1 час.**

Безопасность личной информации. Создание резервных копий на различных устройствах.

**Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 часа.**

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. 3 часа.**

**Повторение. Волонтерская практика. 3 часа.**

**Формы организации:**

- традиционный урок (коллективная и групповая формы работы)
- тренинги (в классической форме или по кейс-методу)
- дистанционное обучение (видеоролики, почтовые рассылки)
- диспуты
- проекты
- общественно-полезные практики

**Виды деятельности**

- Познавательная
- Проблемно-ценностное общение
- Техническое творчество
- Проектная деятельность

Оценивание результативности освоения обучающимися программы внеурочной деятельности «Информационная безопасность» осуществляется с помощью тестирования. (см. Приложение).

**Критерии оценки результатов тестов:**

- 80 – 100% - высокий уровень освоения программы;
- 60-80% - уровень выше среднего;
- 50-60% - средний уровень;
- 30-50% - уровень ниже среднего
- меньше 30% - низкий уровень.

## Тематическое планирование

Согласно плану внеурочной деятельности ГБОУ ООШ № 9 г. Новокуйбышевска на реализацию рабочей программы учебного курса «Информационная безопасность» выделено по 1 часу в неделю в 7-ом, всего по 34 часа в год.

№ п/п	Тема	Количество часов
<b>Тема 1. «Безопасность общения»</b>		
1	Общение в социальных сетях и мессенджерах	1
2	С кем безопасно общаться в интернете	1
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
8	Публичные аккаунты	1
9	Фишинг	2
10	Выполнение и защита индивидуальных и групповых проектов	3
<b>Тема 2. «Безопасность устройств»</b>		
1	Что такое вредоносный код	1
2	Распространение вредоносного кода	1
3	Методы защиты от вредоносных программ	2
4	Распространение вредоносного кода для мобильных устройств	1
5	Выполнение и защита индивидуальных и групповых проектов	3
<b>Тема 3 «Безопасность информации»</b>		
1	Социальная инженерия: распознать и избежать	1
2	Ложная информация в Интернете	1
3	Безопасность при использовании платежных карт в Интернете	1
4	Беспроводная технология связи	1
5	Резервное копирование данных	1
6	Основы государственной политики в области формирования культуры информационной безопасности	2
7	Выполнение и защита индивидуальных и групповых проектов	3
8	Повторение	2
9	Волонтерская практика	1
	Итого	34

**Тест 1**

**Раздел 1 «Безопасность общения»**

**1) Аккаунт социальной сети - это...**

- a) графическое представление пользователя
- b) онлайн-сервис или веб-сайт
- c) учетная запись, личная страница пользователя

**2) Что такое социальная сеть?**

- a) программа для загрузки интернет-страниц
- b) интернет-страница или веб-сайт, позволяющий общаться и обмениваться информацией
- c) учетная запись

**3) Установить соответствие между функциями браузера и их описанием**

- 1) история посещения страниц
  - 2) сохранение паролей
  - 3) управление всплывающими окнами
  - 4) управление информацией о местоположении
  - 5) автозаполнение
- 
- a) упрощает доступ к регулярно посещаемым сайтам за счет автоматического ввода
  - b) автоматическая блокировка всплывающих окон
  - c) возврат на посещенную страницу или восстановление события
  - d) использование данных о местоположении для вывода ближайших запрашиваемых мест
  - e) доступ к регулярно посещаемым сайтам за счет автоматического заполнения учетных данных

**4) Что необходимо для входа в аккаунт?**

- a) инверсия
- b) логин
- c) скриншот
- d) аватар
- e) пароль

**5) Выберите информацию, которую безопасно размещать на своей странице:**

- a) хобби

- b) паспортные данные
- c) местоположение
- d) любимые книги
- e) номер школы
- f) домашний адрес
- g) любимые места в городе

**6) Отметьте простые пароли для использования в учетной записи:**

- a) sqwertb
- b) Tdscg 12\_5v
- c) MyAccc.ert
- d) uipot
- e) eve.try
- f) Reper 1987
- g) Qwasd.13%7

**7) Что такое двухфакторная аутентификация?**

**8) Кибербуллинг – это..**

- a) навязчивое внимание к человеку со стороны другого человека
- b) угрозы, травля, оскорбления в интернете
- c) доступ в режиме реального времени к пользовательскому контенту

**9) Какие настройки конфиденциальности следует установить, чтобы обезопасить себя от мошенников?**

- a) приватность подарков
- b) приватность персональных данных
- c) приватность списка друзей
- d) приватность местоположения
- e) приватность фотографий
- f) приватность аудиозаписей

## Тест 2

### Раздел 2 «Безопасность устройств»

#### 1) Соотнесите названия вредоносных кодов с их описанием:

- 1) вирус
- 2) троян
- 3) червь
- 4) руткиты
- 5) бэкдор
- 6) загрузчик

- a) часть кода, используемая для загрузки и установки вредоносной программы
- b) самовоспроизводящийся вредоносный код
- c) вредоносная программа, которая устанавливается на компьютере отдельным файлом и распространяется через сеть Интернет
- d) вредоносная программа, которая может блокировать, изменять, повреждать, удалять, шифровать данные на устройстве
- e) вредоносная программа, которую после активации трудно обнаружить на устройстве
- f) программа для получение доступа к данным и удаленного управления устройством

#### 2) Что такое расширение?

- a) последовательность букв после точки в названии файла для обозначения его формата
- b) алгоритм для автоматизации каких-то процессов
- c) комплекс программ, предназначенный для управления файлами

#### 3) Как распространяются вредоносные программы?

- a) при посещении популярных сайтов
- b) с помощью вложенных в электронные письма файлов
- c) при авторизации в социальной сети
- d) с помощью файлообменников и торрентов
- e) при переходе по ссылке для подтверждения регистрации
- f) при использовании зараженной интернет страницы

#### 4) Отметьте истинные высказывания

- a) трояны и вирусы распространяются самостоятельно
- b) трояны распространяются самостоятельно, а вирусы распространяют люди
- c) трояны распространяют люди, а вирусы распространяются самостоятельно
- d) трояны и вирусы распространяют люди
- e) черви распространяются самостоятельно

f) черви распространяют люди

**5) Отметьте виды программ, которые всегда вредоносны:**

- a) утилиты
- b) макросы
- c) троян
- d) руткиты
- e) софт
- f) бэкдор
- e) архиватор
- g) скрипт

**6) Что такое спам?**

- a) массовые незапрашиваемые рассылки
- b) вредносный код
- c) вредоносная программа

**7) На какие параметры следует обращать внимание, приобретая антивирусные программы?**

**8) Что такое операционная система (ОС)?**

- a) игровая платформа
- b) комплекс программ, предназначенный для управления ресурсами технического устройства
- c) вспомогательная программа, созданная для выполнения типовых задач

**9) Когда получен спам по e-mail с приложенным файлом, следует:**

- a) прочитать приложение, если оно не содержит ничего ценного – удалить
- b) сохранить приложение в парке «Спам», выяснить IP-адрес генератора спама
- c) удалить письмо с приложением, не раскрывая (не читая) его

**10) Чтобы предотвратить заражение вирусами необходимо:**

- a) регулярное обновление операционной системы
- b) проверка всех ссылок и файлов, полученных по электронной почте
- c) установка только лицензионной версии программного обеспечения
- d) отказ от перехода по ссылкам из всплывающих окон
- e) установка на компьютер сразу нескольких средств защиты
- f) загрузка программного обеспечения только с официальных сайтов разработчиков

## Тест 3

### Раздел 3 «Безопасность информации»

#### 1) Объясните следующие понятия:

- a) фейковый сайт
- b) фейковый аккаунт
- c) фейковые новости
- d) фейковая кредитная карта

#### 2) Что такое СМИ?

- a) распространение ложной информации
- b) процесс несанкционированной активности в инфраструктуре атакуемой системы
- c) совокупность органов публичной передачи информации с помощью технических средств

#### 3) Соедините понятия с их определениями:

- 1) гаджет
- 2) патч
- 3) интерфейс
- 4) VPN (Virtual private network)
- 5) WEP (wired equivalent privacy)
- 6) роутер

- a) виртуальная частная сеть, используемая для доступа к корпоративной сети
- b) прибор, позволяющий настроить сеть Интернет между подключенными к нему устройствами
- c) портативное техническое устройство
- d) алгоритм для обеспечения безопасности сети Wi-Fi
- e) набор инструментов, предназначенный для взаимодействия человека и технического устройства
- f) исправления и дополнения программного кода

#### 4) Для безопасной работы с Wi-Fi в публичном месте необходимо:

- a) по возможности использовать мобильный интернет
- b) выбирать сеть, название которой совпадает с названием заведения
- c) обновлять программные обеспечения из публичных сетей
- d) уточнять у сотрудников сеть, которой лучше воспользоваться
- e) использовать VPN
- f) нажимать продолжить, если появилось объявление об ошибке сертификата
- g) подключаться к сетям без авторизации

#### 5) Какое шифрование, предназначенное для защиты сети, легко взломать?

- a) WEP
- b) WPA
- c) WPA2

**6) Резервное копирование позволяет...**

- a) обезопасить хранимую информацию от повреждений и выхода из строя
- b) защищает информацию от вредоносных программ и вирусов
- c) позволяет восстановить ценную информацию, поврежденную или удаленную на устройстве

**7) Критерии, обеспечивающие безопасность, при использовании интернет-магазинов и совершении онлайн платежей онлайн-платежах**

- a) обновление операционной системы
- b) обновление браузера
- c) компьютер близких родственников
- d) цена на товар значительно ниже среднерыночной цены
- e) антивирусная защита устройства
- f) большое количество исключительно хвалебных отзывов



## Ответы на тесты

### Тест 1

1) с ; 2) b ; 3) 1-с, 2-е, 3-б, 4-д, 5-а ; 4) b, e ; 5) a, d, g ; 6) a, d, e ;

7) логин, пароль и подтверждение через (минимум 2) смс, голосовой вызов, мобильное приложение, наличие устройств: usb-токен, смарт-карта

8) b; 9) b, d, e

### Тест 2

1) 1-б, 2-д, 3-с, 4-е, 5-ф, 6-а; 2) а ; 3) b, d, e, f ; 4) с, е ; 5) с, d, f ; 6) а ;

7) (минимум 5) платность/бесплатность, уровень детектирования (обнаружения вредоносных программ), уровень ложных срабатываний, разнообразие функций (умение работать с вредоносным кодом, фишингом, спамом, предупреждение об обновлениях операционной системы), влияние на скорость работы компьютера, ресурсоемкость, русский язык (русский интерфейс)

8) b ; 9) с ; 10) а, с, d, f

### Тест 3

1) (фейковый — поддельный, фальсифицированный, лживый, фальшивый)

фейковый сайт - фальсифицированный сайт, копия страницы известного сайта

фейковый аккаунт — аккаунт с недостоверной информацией (имя, контакты, фотографии)

фейковые новости — фальшивые новости

фейковая кредитная карта — банковская карта, оформленная на несуществующего человека

2) с ; 3) 1-с, 2-ф, 3-е, 4-а, 5-д, 6-б ; 4) а, d, e ; 5) а ; 6) с ; 7) а, b, e