

**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**муниципальное бюджетное общеобразовательное учреждение**

**"Школа №156" городского округа Самара**

**РАССМОТРЕНО**

Руководитель ШМО  
естественно-  
математического цикла

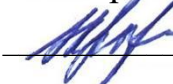


Синёва Н.А.

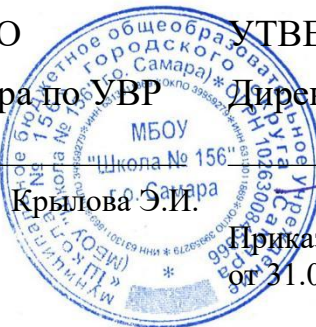
Протокол № 1  
от 28.08.2026 г.

**ПРОВЕРЕНО**

Зам.директора по УВР



28.08.2026 г.



**УТВЕРЖДАЮ**

Директор школы

Крылова Э.И.

Макаров А.С.

Приказ № 320-од  
от 31.08.2026 г.

**РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ  
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

**Уровень образования основное общее: 7 класс**

**Срок реализации программы: 1 год**

**Количество часов: 1 час в неделю**

**Самара 2026**

## **Пояснительная записка**

Рабочая программа курса внеурочной деятельности «**Информационная безопасность**» разработана на основании рабочей программы учебного курса "Информационная безопасность или На расстоянии одного вируса". 7-9 классы. Наместникова М.С. - М.: Просвещение, 2019.

### **Общая характеристика курса внеурочной деятельности**

С каждым годом молодёжи в Интернете становится больше. Социальные сети входят в нашу жизнь, многие люди находятся там постоянно. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями. И поэтому наша жизнь диктует новые требования как к организации самого учебно-воспитательного процесса в средней школе, так и к содержанию образования.

**Основными целями** изучения 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 курса:**

- 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.

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. Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 8 классов.

Система учебных заданий должна создавать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз (составление памяток,

анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы и т.д.).

### **Место учебного курса в учебном плане**

Программа курса внеурочной деятельности рассчитана на 34 учебных часа (по 1 часу в неделю)

### **Содержание курса**

Содержание программы курса внеурочной деятельности соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) 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.

Основное содержание программы представлено разделами:

- «Безопасность общения»,
- «Безопасность устройств»,
- «Безопасность информации».

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

#### **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. Овершаринг.

##### **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.

#### **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.**

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

### **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.**

## **Планируемые результаты**

### ***Предметные:***

*Выпускник научится:*

- анализировать доменные имена компьютеров и адреса документов в интер-нете;
- безопасно использовать средства коммуникации,
- безопасно вести и применять способы самозащиты при попытке мошенни-чества,
- 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.

### ***Метапредметные:***

*Регулятивные универсальные учебные действия.*

В результате освоения учебного курса обучающийся сможет:

- 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.*

В результате освоения учебного курса обучающийся сможет:

- 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.*

В результате освоения учебного курса обучающийся сможет:

- 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.

#### **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; инте-риоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

#### **Формы организации учебной деятельности**

В преподавании курса могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат.

#### **Формами контроля при проведении данного курса являются:**

- тестирование, выборочный опрос, тренировочные задания, анализ работы с текстом;
- самостоятельная работа;
- письменные отчёты по результатам проведённых исследовательских работ;
- защита проектов

#### **Тематическое планирование**

| <b>Тема</b>                                               | <b>Количество часов</b> | <b>Часы аудиторных занятий</b> | <b>Часы активных занятий</b> |
|-----------------------------------------------------------|-------------------------|--------------------------------|------------------------------|
| <b>«Безопасность общения»</b>                             | <b>13</b>               | <b>9</b>                       | <b>4</b>                     |
| Общение в социальных сетях и мессенджерах                 | 2                       | 1                              | 1                            |
| С кем безопасно общаться в интернете                      | 2                       | 1                              | 1                            |
| Пароли для аккаунтов социальных сетей                     | 1                       | 1                              |                              |
| Безопасный вход в аккаунты                                | 1                       | 1                              |                              |
| Настройки конфиденциальности в социальных сетях           | 1                       | 1                              |                              |
| Публикация информации в социальных сетях                  | 2                       | 1                              | 1                            |
| Кибербуллинг                                              | 1                       | 1                              |                              |
| Публичные аккаунты                                        | 1                       | 1                              |                              |
| Фишинг                                                    | 2                       | 1                              | 1                            |
| <b>«Безопасность устройств»</b>                           | <b>8</b>                | <b>4</b>                       | <b>4</b>                     |
| Что такое вредоносный код                                 | 2                       | 1                              | 1                            |
| Распространение вредоносного кода                         | 2                       | 1                              | 1                            |
| Методы защиты от вредоносных программ                     | 2                       | 1                              | 1                            |
| Распространение вредоносного кода для мобильных устройств | 2                       | 1                              | 1                            |
| <b>«Безопасность информации»</b>                          | <b>11</b>               | <b>6</b>                       | <b>5</b>                     |
| Социальная инженерия: распознать и избежать               | 2                       | 1                              | 1                            |

|                                                                                             |           |           |           |
|---------------------------------------------------------------------------------------------|-----------|-----------|-----------|
| Ложная информация в Интернете                                                               | 2         | 1         | 1         |
| Безопасность при использовании платежных карт в Интернете                                   | 2         | 1         | 1         |
| Беспроводная технология связи                                                               | 2         | 1         | 1         |
| Резервное копирование данных                                                                | 2         | 1         | 1         |
| Основы государственной политики в области формирования культуры информационной безопасности | 1         | 1         |           |
| <b>Выполнение и защита индивидуальных проектов</b>                                          | 2         |           | 2         |
| <b>Итого</b>                                                                                | <b>34</b> | <b>19</b> | <b>15</b> |