

Извлечение из организационного раздела  
ООП ООО утвержденных  
приказом директора ГБОУ СОШ № 3 города Похвистнево  
№ 326-од от 31.08.2023 г.

**Программа**  
**курса внеурочной деятельности**  
**«Информационная безопасность»**  
( ВД по обеспечению безопасности  
жизни и здоровья обучающихся)  
для 8 класса

Рассмотрено и рекомендовано к утверждению  
на заседании МО классных руководителей:  
Протокол № 1 от 28.08.2023

Составлена  
классными руководителями 8-ых классов

Проверено  
заместителем директора по УВР  
Хмелевой В.В.

## Пояснительная записка

Рабочая программа курс «Информационная безопасность» для обучающихся 7—9 классов составлена в соответствии с Федеральным государственным образовательным стандартом основного общего образования, на основе Примерной рабочей программы учебного курса «Цифровая гигиена» основного общего образования, рекомендованной Координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019). Самара, 2019.

### Цель программы:

- формирование активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им;
- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз.

### 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.

### Общая характеристика курса.

Данный курс предполагает организацию работы в соответствии с содержанием 2-х модулей, предназначенных для обучающихся 8 классов и родителей обучающихся любого возраста соответственно.

**Модуль 1. «Информационная безопасность»** реализуется в рамках внеурочной деятельности обучающихся. Программа рассчитана на 17 часов.

### Планируемые результаты обучения

#### Предметные:

*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.

## **Метапредметные.**

### **Регулятивные универсальные учебные действия.**

*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.**

*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.**

*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; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

## **Содержание курса**

Содержание программы курса соответствует темам основной образовательной программы основного общего образования (ООП 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 учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

| № | Раздел                    | Количество часов |
|---|---------------------------|------------------|
| 1 | «Безопасность общения»    | 8                |
| 2 | «Безопасность устройств»  | 4                |
| 3 | «Безопасность информации» | 5                |

## **Содержание программы. Модуль 1. «Информационная безопасность»**

### **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.

### **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. 1 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. Беспроводная технология связи. 1 час.**

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

**Тема 4. Резервное копирование данных. 1 час.**

Безопасность личной информации. Создание резервных копий на различных устройствах.

**Тема 5. Основы государственной политики в области формирования культуры информационной безопасности. 1 часа.**

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

### Тематическое планирование

| №                                       | Тема   | Основное содержание   | Кол-во часов | Характеристика основных видов учебной деятельности обучающихся  |
|---|--|---|--------------|---|
| <i>Раздел 1. «Безопасность общения»</i> |  |   |              |   |
| 1                                       | Тема 1. Общение в социальных сетях и мессенджерах.       | Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.   | 1            | Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет. |
| 2                                       | 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. | 1            | Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.   |
| 3                                       | Тема 3. Пароли для аккаунтов социальных сетей.           | Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.   | 1            | Изучает основные понятия регистрационной информации и шифрования. Умеет их применять.   |
| 4                                       | Тема 4. Безопасный вход в аккаунты.                      | Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.  | 1            | Объясняет причины безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.   |
| 5                                       | Тема 5. Настройки конфиденциальности в социальных сетях. | Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.  | 1            | Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.   |
| 6                                       | Тема 6. Публикация информации в социальных               | Персональные данные. Публикация   | 1            | Осуществляет поиск и использует   |

|   |                             |   |   |   |
|---|-----------------------------|---|---|---|
|   | сетях.                      | личной информации.  |   | информацию, необходимую для выполнения поставленных задач.  |
| 7 | Тема 7. Кибербуллинг.       | Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. | 1 | Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.   |
| 8 | Тема 8. Публичные аккаунты. | Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.   | 1 | Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности. |

*Раздел 2. «Безопасность устройств»*

|    |  |  |   |   |
|----|--|--|---|---|
| 14 | Тема 1. Что такое вредоносный код          | Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.   | 1 | Соблюдает технику безопасности при эксплуатации компьютерных систем.          |
| 15 | Тема 2. Распространение вредоносного кода. | Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия | 1 | Выявляет и анализирует возможные угрозы информационной безопасности объектов. |

|    |  |   |   |  |
|----|--|---|---|--|
|    |  | вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.                                    |   |  |
| 16 | Тема 3. Методы защиты от вредоносных программ. | Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов. | 1 | Изучает виды антивирусных программ и правила их установки. |



|   |  |   |    |   |
|---|--|---|----|---|
| 17  | Тема 4. Распространение вредоносного кода для мобильных устройств.                                   | Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.  | 1  | Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.   |
| <i>Раздел 3 «Безопасность информации»</i> |  |   |    |   |
| 18  | Тема 1. Социальная инженерия: распознать и избежать.   | Приемы социальной инженерии. Правила безопасности при виртуальных контактах.  | 1  | Находит нужную информацию в базах данных, составляя запросы на поиск.   |
| 19  | Тема 2. Ложная информация в Интернете.   | Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.   | 1  | Определяет возможные источники необходимых сведений, осуществляет поиск информации.   |
| 20  | Тема 4. Беспроводная технология связи.   | Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.  | 1  | Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.   |
| 21  | Тема 5. Резервное копирование данных.  | Безопасность личной информации. Создание резервных копий на различных устройствах.  | 1  | Создает резервные копии.  |
| 22  | 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. | 1  | Умеет привести выдержки из законодательства РФ: обеспечивающего конституционное право на поиск, получение и распространение информации. Отражающего правовые аспекты защиты киберпространства |
|   | Итого  |   | 17 |   |

## Список источников

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019 – 432 с
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014 – 182 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017 – 384 с.
4. Дети в информационном обществе <http://detionline.com/journal/about>
5. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ- ДАНА, 2016 – 239 с.
6. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018 – 558 с.
7. Защита детей by Kaspersky // <https://kids.kaspersky.ru/>
8. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017 – 64 с.
9. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019 – 80 с.
10. Основы кибербезопасности. // <https://www.xn--d1abkefqip0a2f.xnplai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kurs>
11. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013 – 144 с.