

**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**государственное бюджетное общеобразовательное учреждение Самарской**  
**области основная общеобразовательная школа пос. Пензено муниципального**  
**района Большечерниговский Самарской области**

**Самарская область**  
**ГБОУ ООШ пос. Пензено**

РАССМОТРЕНО  
на заседании МО

\_\_\_\_\_  
С.В. Сульдина  
от «29» 08 2024 г.

СОГЛАСОВАНО  
Заместитель директора по  
УВР

\_\_\_\_\_  
С.В. Сульдина  
от «29» 08 2024 г.

УТВЕРЖДЕНО  
Директор ГБОУ ООШ п.  
Пензено

\_\_\_\_\_  
В.А. Ишуков  
Приказ № 92-од  
от «29» 08 2024 г.

**РАБОЧАЯ ПРОГРАММА**  
**внеурочной деятельности**

**«Информационная безопасность»**

для обучающихся 7 класса

**п. Пензено**  
**2024 г.**

## Общая характеристика курса внеурочной деятельности

### Пояснительная записка

Программа курса «Цифровая гигиена» адресована учащимся 7 классов и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным результатам.

### Актуальность программы.

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.

Данный курс предполагает организацию работы в соответствии с содержанием, предназначенных для обучающихся 7 классов.

**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 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.

### Место курса внеурочной деятельности в основной образовательной программе ГБОУ ООШ п.Пензено

Рабочая программа курса «Информационная безопасность» для 7 класса является приложением к Основной общеобразовательной программе основного общего образования ГБОУ ООШ п.Пензено на 2024-2025 учебный год, соответствует годовому календарному учебному графику ГБОУ ООШ п.Пензено на 2024-2025 учебный год.

Программа курса рассчитана на 1 год – 34 часа, по 1 часу в неделю.

### ***Итоговый контроль:***

Оценивание деятельности по курсу происходит в форме «зачёт» за каждый пройденный раздел:

- «зачёт» Знания, умения, навыки соответствуют программным требованиям в полном/полном объёме
- «незачёт» Программа не освоена, программные требования не выполнены.

## **Характеристика личностных, метапредметных и предметных результатов освоения учебного курса.**

### ***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.*

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

## **Содержание программы учебного курса.**

Содержание программы учебного курса 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 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.

## **Содержание учебного курса**

### **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. 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. 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.**

### Тематическое планирование учебного курса.

№ п.п	Тема занятия	Кол-во часов		ЦОР
		теоретич	практич	
	<b>Тема 1. «Безопасность общения» (13 ч.)</b>	<b>6</b>	<b>7</b>	
1	Общение в социальных сетях и мессенджерах	1	-	
2	С кем безопасно общаться в интернете	1	-	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
3	Пароли для аккаунтов социальных сетей	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
4	Безопасный вход в аккаунты	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
5	Настройки конфиденциальности в социальных сетях	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
6	Публикация информации в социальных сетях	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
7	Кибербуллинг	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
8	Публичные аккаунты.	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
9	Фишинг	1	1	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
10	Выполнение и защита индивидуальных и групповых проектов	-	3	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
	<b>Тема 2. «Безопасность устройств» (8 ч.)</b>	<b>2,5</b>	<b>5,5</b>	
11	Что такое вредоносный код	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
12	Распространение вредоносного кода	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
13	Методы защиты от вредоносных программ	1	1	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
14	Распространение вредоносного кода для мобильных устройств	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
15	Выполнение и защита индивидуальных и групповых проектов	-	3	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
	<b>Тема 3 «Безопасность информации» (13 ч.)</b>	<b>4,5</b>	<b>8,5</b>	
16	Социальная инженерия: распознать и избежать	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
17	Ложная информация в Интернете	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
18	Безопасность при использовании платежных карт в Интернете	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
19	Беспроводная технология связи	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
20	Резервное копирование данных	0,5	0,5	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
21	Основы государственной политики в области формирования культуры информационной безопасности	2	-	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
22	Выполнение и защита индивидуальных и групповых проектов	-	3	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
23	Повторение, волонтерская практика	-	3	<a href="http://penzenodist.minobr63.ru/">http://penzenodist.minobr63.ru/</a>
	<b>Итого</b>	<b>13</b>	<b>21</b>	

**Требования к содержанию итоговых проектно-исследовательских работ***Критерии содержания текста проектно-исследовательской работы*

1. Во введении сформулирована актуальность (личностная и социальная значимость) выбранной проблемы. Тема может быть переформулирована, но при этом четко определена, в необходимости исследования есть аргументы.
2. Правильно составлен научный аппарат работы: точность формулировки проблемы, четкость и конкретность в постановке цели и задач, определении объекта и предмета исследования, выдвижении гипотезы. Гипотеза сформулирована корректно и соответствуют теме работы
3. Есть планирование проектно-исследовательской деятельности, корректировка ее в зависимости от результатов, получаемых на разных этапах развития проекта. Дана характеристика каждого этапа реализации проекта, сформулированы задачи, которые решаются на каждом этапе, в случае коллективного проекта – распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведен корректно
4. Используется и осмысливается междисциплинарный подход к исследованию и проектированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников
5. Определён объём собственных данных и сопоставлено собственное проектное решение с аналоговыми по проблеме. Дан анализ источников и аналогов с точки зрения значимости для собственной проектно-исследовательской работы, выявлена его новизна, библиография и интернет ресурсы грамотно оформлены
6. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.
7. Есть оценка результативности проекта, соотнесение с поставленными задачами. Проведена оценка социокультурных и образовательных последствий проекта на индивидуальном и общественном уровнях.

*Критерии презентации проектно-исследовательской работы (устного выступления)*

1. Демонстрация коммуникативных навыков при защите работы. Владение риторическими умениями, раскрытие автором содержание работы, достаточная осведомленность в терминологической системе проблемы, отсутствие стилистических и речевых ошибок, соблюдение регламента.
2. Умение чётко отвечать на вопросы после презентации работы.
3. Умение создать качественную презентацию. Демонстрация умения использовать IT-технологии и создавать слайд презентацию на соответствующем его возрасту уровне.
4. Умение оформлять качественный презентационный буклет на соответствующем его возрасту уровне.
5. Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видео-ролик, мультфильм и т.д.).
6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность наметить пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации коммуникабельности, благодарности и уважения по отношению к руководителю, консультантам, умение четко обозначить пути создания сетевого продукта.
7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.



### **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.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa>
11. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.
12. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон. научн. журн. 2019. № 22(66)
13. 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.