**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Министерство образования и науки Смоленской области**

**Администрация города Смоленска**

Капаёва Любовь Валерьевна
Подписано цифровой подписью: Капаёва Любовь Валерьевна
Дата: 2024.11.04 14:06:53 +03'00'

**МБОУ "Гимназия № 4"**

| РАССМОТРЕНО | СОГЛАСОВАНО | УТВЕРЖДЕНО |
|---|---|---|
| на заседании кафедры | на заседании педагогического совета | приказом директора МБОУ "Гимназия 4" |
| руководитель кафедры | | |
| _____ | _____ | _____ |
| А.Т. Романова | Протокол №1 от «30» августа 2024 г. | Капаева Л.В. |
| Протокол №1 от «30» августа 2024 г. | | Приказ №32-од от «30» 08 2024 г. |

# РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

**(ID 6125102)**

**Информационная безопасность**

для обучающихся 7 классов

**Смоленск 2024**

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

ОБЩАЯ ХАРАКТЕРИСТИКА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

Курс внеурочной деятельности «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.

ЦЕЛИ ИЗУЧЕНИЯ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

Цели:

- 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);
- 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, изобрази-тельных, 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.

Категория обучающихся – 13-15 лет
Срок реализации программы – 1 год
Режим занятий – 1 раз в неделю по 2 часа.

## МЕСТО КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ "ИНФОРМАЦИОННАЯ БЗОПАСНОСТЬ" В ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Программа учебного курса рассчитана на 72 учебных часа, из них 60 часов – учебные занятия, 9 часов –подготовка и защита учебных проектов, 3 часа – повторение. На изучение курса внеурочной деятельности «Информационная безопасность» отводится по 2 часа в неделю.

## ФОРМЫ ПРОВЕДЕНИЯ ЗАНЯТИЙ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

Формы организации деятельности: групповая, индивидуальная, индивидуально - групповая (3-5 человек).
Занятия проводятся в комбинированной, теоретической и практической форме:

- теоретические занятия: основы безопасного поведения при работе с компьютерными программами, информацией в сети интернет, изучение терминов, беседы, лекции;
- практические занятия: работа с мобильными устройствами;
- создание буклетов и мультимедийных презентаций.

## СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

Содержание программы курса внеурочной деятельности соответствует темам по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», 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. Предусмотрено оценивание достижений обучающихся по системе «зачѐт - незачѐт». Промежуточная аттестация проводится в форме проекта.

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. Овершеринг.

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. 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. Повторение. Волонтерская практика.

## ПЛАНИРУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

- 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 РЕЗУЛЬТАТЫ

- 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;

• 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.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

• 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;

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

• 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.

## ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

| № п/п | Наименование разделов и тем программ | Количество часов | Основное содержание | Основные виды деятельности | Электронные (цифровые) образовательные ресурсы |
|---|---|---|---|---|---|
| 1 | Общение в социальных сетях и мессенджерах | 2 | Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент. | Познавательная деятельность | |
| 2 | С кем безопасно общаться в интернете | 2 | Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети | Познавательная деятельность | |
| 3 | Пароли для аккаунтов социальныхсетей | 4 | Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей. | Познавательная деятельность | |
| 4 | Безопасный вход в аккаунты | 2 | Виды аутентификации. Настройки безопасности аккаунта. Работа | Познавательная деятельность | |

| | | | | | |
|---|---|---|---|---|---|
| | | | на чужом компьютере сточки зрения безопасности личного аккаунта | | |
| **5** | Настройки конфиденциальности в социальных сетях | **4** | Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах. | Познавательная деятельность | |
| **6** | Публикация информации в социальных сетях | **6** | Персональные данные. Публикация личной информации | Познавательная деятельность | |
| **7** | Кибербуллинг | **4** | Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. | Познавательная деятельность | |
| **8** | Публичные аккаунты | **4** | Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг. | Познавательная деятельность | |
| **9** | Фишинг | **10** | Фишинг как мошеннический прием. | Познавательная деятельност | |

| | | | | | |
|---|---|---|---|---|---|
| | | | Популярныевариа нты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетяхи мессенджерах. | ь | |
| **Тема 2. «Безопасность устройств»** | | | | | |
| **1** | Что такое вредоносный код? | **2** | Виды вредоносных кодов. Возможности и Деструктивные функции вредоносных кодов. | Познавател ьная деятельност ь | |
| **2** | Распростра нение вредоносного кода | **4** | Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. | Познавател ьная деятельност ь | |
| **3** | Методы защиты от вредоносных программ | **2** | Способы защиты устройств от вредоносногокода . Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов | Познавател ьная деятельност ь | |
| 4 | Распространение | **8** | Расширение | Познавател | |

| | | | | | |
|---|---|---|---|---|---|
| | вредоносного кода для мобильных устройств | | вредоносных кодов для мобильныхустройств. Правила безопасности при установке приложений на мобильные устройства. | ьная деятельность | |
| **Тема 3 «Безопасность информации»** | | | | | |
| **1** | Социальная инженерия: распознать и избежать | **2** | Приемы социальной инженерии. Правила безопасности при виртуальных контактах. | Познавательная деятельность | |
| **2** | Ложная информация в Интернете | **2** | Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы. | Познавательная деятельность | |
| **3** | Безопасность при использовании платежных карт в Интернете | **2** | Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов. | Познавательная деятельность | |
| **4** | Беспроводная технология связи | **4** | Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в | Познавательная деятельность | |

| | | | | | |
|---|---|---|---|---|---|
| | | | публичных сетях. | | |
| **5** | Резервное копирование данных | **2** | Безопасность личной информации. Создание резервных копий на различных устройствах. | Познавательная деятельность | |
| **6** | Основы Государственно й политики в области формирования культуры информационной безопасности | **6** | Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности. | Познавательная деятельность | |
| **Итого:** | | **72 часа** | | | |