**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ГОРОДСКОГО ОКРУГА ТОЛЬЯТТИ**

**«ШКОЛА № 90»**



Пояснительная записка

Курс внеурочной деятельности «Информационная безопасность» **разработана с учетом требований следующих нормативно-правовых актов**:

Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями);

Приказ Министерства просвещения Российской Федерации от 27.07.2022 № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

Концепция развития дополнительного образования детей до 2030 года, утвержденная распоряжением Правительства Российской Федерации № 678-р от 31.03.2022;

Постановление Главного государственного санитарного врача РФ от 28.09.2020 № 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи».

Устав МБОУ «Орджоникидзевская СОШ»;

Положение о внеурочной деятельности МБОУ «Орджоникидзевская СОШ»

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**:

1. 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);
2. 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;
3. 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.;
4. 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;
5. сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

**Общая характеристика учебного курса**

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.

Программа учебного курса (Модуль 1) рассчитана на 34 учебных часа, из них 22 часа - учебных занятий, 9 часов - подготовка и

защита учебных проектов, 3 часа - повторение. На изучение курса внеурочной деятельности «Информационная безопасность» отводится по 1 часу в неделю в 8 классе и 1 час в неделю в 9 классе.

**Личностные, метапредметные и предметные результаты 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 иформальных 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 познава-тельных 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**

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

Каждый раздел курса внеурочной деятельности завершается выполнением проектной работы по одной из тем, предложенных навыбор 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. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные входе выполненияучебных заданий по основным темам 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 жертвойки 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 проектов3. 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 час**

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 без-опасности 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 час.**

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации 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**

**курса внеурочной деятельности «Информационная безопасность» в 8 - 9 классах**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  п/ п | Тема | Кол- во часов | Пр им ер ны  е сро ки пр ове де ни  я | Основное содержание | Характеристика основных видов учебной деятельности обучающихся |
| **Тема 1. «Безопасность общения»** | | | | | |
| 1 | Общение в социальных сетяхи мессенджерах | 1 |  | Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров.  Пользовательский контент. | 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 | С кем безопасно общаться винтернете | 1 |  | Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя.  Анонимные социальные сети. | Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения. |
| 3 | Пароли для аккаунтов социальных сетей | 1 |  | Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование  функции браузера по запоминанию паролей. | Изучает основные понятия регистрационной информации и шифрования. Умеет их применить. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 4 | Безопасный вход в аккаунты | 1 |  | Виды аутентификации. Настройки безопасности  аккаунта. Работа на чужом компьютере с точки зрения  безопасности личного аккаунта. | Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа. |
| 5 | Настройки конфиденциаль ности в социальных сетях | 1 |  | Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах. | Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле. |
| 6 | Публикация информации в социальных сетях | 1 |  | Персональные данные. Публикация личной информации. | Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач. |
| 7 | Кибербуллинг | 1 |  | Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. | Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников. |
| 8 | Публичные аккаунты | 1 |  | Настройки приватности публичных страниц.  Правила ведения публичных страниц. Овершеринг. | Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности. |
| 9 | Фишинг | 2 |  | Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов.  Как защититься от фишеров в социальных сетях и мессенджерах. | Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек- листа (памятки) по противодействию фишингу. |
| 10 | Выполнение и защита индивидуальны х и групповых проектов | 3 |  |  | Самостоятельная работа. |
| **Тема 2. «Безопасность устройств»** | | | | | |
| 1 | Что такое вредоносный код? | 1 |  | Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов. | Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2 | Распростра нение вредоносно го кода | 1 |  | 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. | Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов. |
| 3 | Методы защиты от вредоносных программ | 2 |  | Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики.  Правила защиты от вредоносных кодов. | Изучает виды антивирусных программ и правила их установки. |
| 4 | Распространение вредоносного кода для мобильных устройств | 1 |  | Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке  приложений на мобильные устройства. | Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся  более младшего возраста. |
| 5 | Выполнение и защита индивидуальн ых и групповых проектов | 3 |  |  | Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты;  гипотезы, аксиомы, теории. |
| **Тема 3 «Безопасность информации»** | | | | | |
| 1 | Социальная инженерия: распознать и избежать | 1 |  | Приемы социальной инженерии. Правила безопасности при виртуальных контактах. | Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска. |
| 2 | Ложная информация в  Интернете | 1 |  | Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей.  Фейковые новости. Поддельные страницы. | Определяет возможные источники необходимых сведений, осуществляет поиск информации.  Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 | Безопасность при использовании платежныхкарт в Интернете | 1 |  | Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов. | Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежныхкарт в Интернете. |
| 4 | Беспроводная технологиясвязи | 1 |  | Уязвимость Wi-Fi-соединений. Публичные и непубличные сети.  Правила работы в публичных сетях. | Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов. |
| 5 | Резервное копирование  данных | 1 |  | Безопасность личной информации. Создание резервных копий на различных устройствах. | Создает резервные копии. |
| 6 | Основы государственной политики в области формирования культуры информационной безопасности | 2 |  | Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности. | Умеет привести выдержки из законодательства РФ:   * обеспечивающего конституционное право на поиск, получение и распространение информации; * отражающего правовые аспекты защиты киберпространства. |
| 7 | Выполнение и защита индивидуальных и групповыхпроектов | 3 |  |  | Самостоятельная и групповая работа по созданию продукта проекта |
| 8 | Повторение, волонтерская практика, резерв | 3 |  |  |  |
| **Итого:** | | **34**  **часа** |  | | |

**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 естьаргументы.
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.

1. Используется и осмысляется междисциплинарный подход к исследованию и проектированию и набазовом уровне школьной программы, и на уровне освоения дополнительных библиографических

источников.

1. Определён объём собственных данных и сопоставлено собственное проектное решение с аналоговыми попроблеме. Дан анализ источников и аналогов с точки зрения значимости для собственной проектно­Исследовательской работы, выявлена его новизна, библиография и интернет ресурсы грамотно оформлены.
2. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.
3. Есть оценка результативности проекта, соотнесение с поставленными задачами. Проведенаоценка 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, раскрытиеавтором 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 создаватьслайд 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 намечать 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.

1. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.