МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования и науки Республики Хакасия
Управление образования Орджоникидзевского района
МБОУ "Июсская СОШ "

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 52141D5872AD68D2DAC08603D43A8932
Владелец: МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "ИЮССКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА"
Действителен: с 13.09.2024 до 07.12.2025

Утверждаю директор
МБОУ «Июсская СОШ»
_____Михайлова Т. С.
Приказ № 100 от30.08.2024г.

РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности

Название «Информационная безопасность»
Направление Занятия, направленные на удовлетворение социальных интересов и потребностей обучающихся, на педагогическое сопровождение деятельности социально ориентированныхученгических сообществ, детских общественных объединений, органов ученического самоуправления, на организацию совместно с обучающимися комплекса мероприятий воспитательной направленности
Класс 5-7

с. Июс 2024

Пояснительная записка

Программа курса внеурочной деятельности курс «Информационная безопасность» адресована обучающимся 5-7 классов и направлена на достижение планируемых предметных, метапредметных и личностных результатов Государственных образовательных стандартов основного и среднего образования.

Курс является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры и т.п.), задумывающимися о своей личной безопасности, безопасности своей семьи и своих друзей, а также проявляющими интерес к изучению истории и технологических основ информационной безопасности.

Курс «Информационная безопасность» рассчитан на 1 год обучения (34 часа). Направление программы - общекультурное.

Программа ориентирована на выполнение требований к организации и содержанию внеурочной деятельности. Ее реализация дает возможность раскрытия индивидуальных способностей обучающихся, развития интереса к различным видам индивидуальной и групповой деятельности, поощрения желания активно участвовать в продуктивной деятельности, умения самостоятельно организовать свою учебную, в том числе проектную деятельность.

Цель программы: формирование активной позиции обучающихся 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 развитии информационной культуры обучающихся, повышения защищённости детей от информационных рисков и угроз.

Задачи программы:

-дать представление о современном информационном обществе, информационной безопасности личности и государства;

-сформировать навыки ответственного и безопасного поведения в современной информационно-телекоммуникационной среде;

-сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом;

-сформировать общекультурные навыки работы с информацией (умений грамотно пользоваться источниками информации, правильно организовывать информационный процесс);

-дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;

-познакомить со способами защиты от противоправных посягательств в Интернете, защиты личных данных.

Планируемые результаты освоения курса

Изучение курса «Информационная безопасность» обусловливает достижение следующих **результатов личностного развития**:

- 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 ценности безопасного образа жизни; формирование правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде

Метапредметные результаты

В ходе изучения учебного курса, обучающиеся усовершенствуют опыт проектной деятельности, и навыки работы с информацией, в том числе в текстовом, табличном виде, виде диаграмм и пр. 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.

Предметные универсальные учебные действия

Научатся:

- 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.

П*олучат возможность овладеть:*

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

-основами соблюдения норм информационной этики и прав;

-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.

Содержание программы внеурочной деятельности

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

Раздел 1. «Безопасность общения» (13 ч)

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).

Раздел 2. «Безопасность устройств» (8ч)

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 устройств).

Раздел 3 «Безопасность информации» (10 ч)

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).

Повторение (3 ч)

Система заданий предполагает индивидуальную и групповую формы работы, составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы.

Каждый раздел программы завершается выполнением теста или проектной работы по предложенным темам.

Тематическое планирование

№	Название раздела (темы)	Количество часов, отведенных на изучение
		Всего
1	Безопасность общения	15
2	Безопасность устройств	9
3	Безопасность информации	10
	ВСЕГО	34 часа

Календарно-тематическое планирование курса внеурочной деятельности «Информационная безопасность»

№ п/п	Тема урока	Дата проведения		Примечание
		по плану	по факту	
1.	Что такое Интернет?	04.09		
2.	Общение в социальных сетях и мессенджерах	11.09		
3.	С кем безопасно общаться в интернете	18.09		
4.	Пароли для аккаунтов социальных сетей	25.09		
5.	Безопасный вход в аккаунты	02.10		
6.	Настройки конфиденциальности в социальных сетях	09.19		
7.	Публикация информации в социальных сетях	16.10		
8.	Кибербуллинг	23.10		
9.	Публичные аккаунты	06.11		
10.	Фишинг	13.11		
11.	Выполнение теста «Безопасность общения»	20.11		
12.	Выполнение и защита индивидуальных и групповых проектов	27.11		
13.	Выполнение и защита индивидуальных и групповых проектов	04.12		
14.	Выполнение и защита индивидуальных и групповых проектов	11.12		
15.	Выполнение и защита индивидуальных и групповых проектов	18.12		
16.	Что такое вредоносный код	25.12		
17.	Распространение вредоносного кода	15.01		
18.	Методы защиты от вредоносных программ	22.01		
19.	Распространение вредоносного кода для мобильных устройств	29.01		
20.	Выполнение теста «Безопасность устройств»	04.02		

№ п/п	Тема урока	Дата проведения		Примечание
		по плану	по факту	
21.	Выполнение и защита индивидуальных и групповых проектов	11.02		
22.	Выполнение и защита индивидуальных и групповых проектов	18.02		
23.	Выполнение и защита индивидуальных и групповых проектов	25.02		
24.	Выполнение и защита индивидуальных и групповых проектов	05.03		
25.	Социальная инженерия: распознать и избежать	12.03		
26.	Ложная информация в Интернете	19.03		
27.	Безопасность при использовании платежных карт в Интернете	26.03		
28.	Беспроводная технология связи	09.04		
29.	Резервное копирование данных	16.04		
30.	Выполнение теста «Безопасность информации»	23.04		
31.	Выполнение и защита индивидуальных и групповых проектов	07.05		
32.	Выполнение и защита индивидуальных и групповых проектов	14.05		
33.	Выполнение и защита индивидуальных и групповых проектов	21.05		
34.	Выполнение и защита индивидуальных и групповых проектов	28.05		