Аннотация к рабочей программе курса внеурочной деятельности «Информационная безопасность или на расстоянии одного вируса» для 7класса

Название программы	Срок	Перечень нормативных правовых актов, регламентирующих разработку рабочей программы учебного предмета/ учебного курса (в том числе внеурочной деятельности)/ учебного модуля
Рабочая программа курса внеурочной деятельности «Информационная безопасность» для 7 класса	1 год	- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»; - Приказ Минпросвещения РФ от 22.03.2021 № 115 «Об утверждении Порядка организации и осуществления образовательной деятельности по основным общеобразовательным программам - образовательным программам начального общего, основного общего и среднего общего образования»; - Указ Президента Российской Федерации от 9.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей». - Приказ Министерства просвещения Российской Федерации от 31.05.2021 № 287 «Об утверждении федерального государственного образовательного стандарта основного общего образования» (Зарегистрирован 05.07.2021 № 64101). - Приказ Министерства просвещения Российской Федерации от 18.07.2022 № 568 «О внесении изменений в федеральный государственный образовательный стандарт основного общего образования» (Зарегистрирован 17.08.2022 № 69675). - Приказ Министерства просвещения Российской Федерации от 19.02.2024 № 110 «О внесении изменений в некоторые приказы Министерства образования и науки Российской Федерации и Министерства просвещения Российской Федерации, касающиеся федеральных государственных образовательных стандартов основного общего образования» (Зарегистрирован 22.02.2024 № 77331). - Приказ Министерства просвещения Российской Федерации от 19.03.2024 № 171 «О внесении изменений в некоторые приказы Министерства просвещения Российской Федерации, касающиеся федеральных образовательных программ начального общего образования, основного общего образования и среднего общего образования» (Зарегистрирован 11.04.2024 № 77830). - Приказ Министерства просвещения Российской Федерации от 22.01.2024 № 31 «О внесении изменений в некоторые приказы Министерства образования и науки Российской Федерации и Министерства просвещения Российской Федерации, касающиеся федеральных государственных образовательных стандартов начального общего образования и основного общего образования» (зарегистрирован в Минюсте России 22 февраля 2024 г., регистрационный № 77330) - Приказ Минпросвещения России от 17 июля 2024 г. № 495 «О внесении изменений в некоторые приказы Министерства просвещения Российской Федерации, касающиеся федеральных адаптированных образовательных программ» (зарегистрирован в Минюсте России 15 августа 2024 г., регистрационный № 79163) - Программа воспитания ГБОУ СОШ с. Калиновка

государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа с. Калиновка муниципального района Сергиевский Самарской области
ГБОУ СОШ с.Калиновка

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
на заседании методического объединения	И.о.заместителя директора по УВР	И.о.директора
Руководитель МО _____	_____Дрогунова И.А.	_____Козлов Н.Н.
Богданова Н.В. Протокол № 4 от «10» мая 2024 г.	Протокол № 4 от «27» июня 2024 г.	Приказ 190-од от 29.08.2024г

C=RU, O=ГБОУ СОШ с. Калиновка, CN=Н.Н. Козлов, E=su.kalinov_sch@63edu.ru место подписания 2025.02.04 11:

РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

«Информационная безопасность»

7 класс

с.Калиновка, 2024 г.

Результаты освоения курса внеурочной деятельности

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.

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 результаты

Регулятивные УУД:

- 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 получениязапланированных характеристик продукта/результата;
- принимать решение в учебной ситуации и нести за него ответственность.

Познавательные УУД

- 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 УУД

- 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 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.

Каждый раздел учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста, что и будет являться контролирующим материалом для оценки планируемых результатов освоения программы.

Содержание программы учебного курса

Содержание программы соответствует требованиям к образовательным результатам освоения ООП ООО ГБОУ СОШ «ОЦ» пос. Серноводск, 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».

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.

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 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 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	Раздел, тема курса	Кол-во часов		Материально-техническое, информационное обеспечение
		Теория	Практика	
Раздел 1. «Безопасность общения»				
1	Общение в социальных сетях и мессенджерах	1	0	• интерактивная доска
2	С кем безопасно общаться в интернете	1	0	• интерактивная доска
3	Пароли для аккаунтов социальных сетей	0	1	• интерактивная доска • нетбуки ученические
4	Безопасный вход в аккаунты	1	0	• интерактивная доска
5	Настройки конфиденциальности в социальных сетях	0	1	• интерактивная доска • нетбуки ученические
6	Публикация информации в социальных сетях	1	0	• интерактивная доска
7	Кибербуллинг	1	0	• интерактивная доска
8	Публичные аккаунты	1	0	• интерактивная доска
9	Фишинг	2	0	• интерактивная доска
10	Выполнение и защита индивидуальных и групповых проектов	1	2	• интерактивная доска • нетбуки ученические
Раздел 2. «Безопасность устройств»				
1	Что такое вредоносный код?	1	0	• интерактивная доска
2	Распространение вредоносного кода	1	0	• интерактивная доска
3	Методы защиты от вредоносных программ	1	1	• интерактивная доска • нетбуки ученические
4	Распространение вредоносного кода для мобильных устройств	1	0	• интерактивная доска
5	Выполнение и защита индивидуальных и групповых проектов	1	2	• интерактивная доска • нетбуки ученические
Раздел 3 «Безопасность информации»				
1	Социальная инженерия: распознать и избежать	1	0	• интерактивная доска
2	Ложная информация в Интернете	1	0	• интерактивная доска
3	Безопасность при использовании платежных карт в Интернете	1	0	• интерактивная доска

4	Беспроводная технология связи	1	0	• интерактивная доска
5	Резервное копирование данных	0	1	• интерактивная доска • нетбуки ученические
6	Основы государственной политики в области формирования культуры информационной безопасности	2	0	• интерактивная доска
7	Выполнение и защита индивидуальных и групповых проектов	1	2	• интерактивная доска • нетбуки ученические
8	Повторение, волонтерская практика, резерв	0	3	• интерактивная доска • нетбуки ученические
Итого:		**21**	**13**	**34 часа**