

Рассмотрена	Проверена	Утверждена
На заседании МО учителей	заместитель директора по	приказом
Музыки, ОБЖ, физкультуры, технологии,	УВР	№ 460/ОД от 31.08.2020
Предметов духовно-нравственной	Симонова Ю.В.	Директор ГБОУ СОШ №3
Направленности		г. Сызрани
Протокол №1		Симонова Т.П.
От «31» августа 2020 г.		

**Рабочая программа внеурочной деятельности
«Информационная безопасность»
(7, 8, 9 классы)**

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа по курсу внеурочной деятельности «Информационная безопасность» для 7-9 классов разработана в соответствии с требованиями Федерального государственного образовательного стандарта основного общего образования, ООП ООО и плана внеурочной деятельности ГБОУ СОШ №3 г. Сызрани.

Составлена на основе программы:

Информационная безопасность Рабочая программа на основе примерной программы учебного курса "Цифровая гигиена". Рек. коорд. Советом УМО Самарской области, Самара, 2019г

Программа курса внеурочной деятельности «Информационная безопасность» рассчитана на 34 учебных часа, из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение в объеме 1 часа в неделю в 7 или в 8 или в 9 классе.

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 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 КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ С УКАЗАНИЕМ ФОРМ ОРГАНИЗАЦИИ И ВИДОВ ДЕЯТЕЛЬНОСТИ

7-9 класс (34 ч)

Безопасность общения

Общение в социальных сетях и мессенджерах. Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

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.

Пароли для аккаунтов социальных сетей. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Безопасный вход в аккаунты. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Настройки конфиденциальности в социальных сетях. Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Публикация информации в социальных сетях. Персональные данные. Публикация личной информации.

Кибербуллинг. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Публичные аккаунты. Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

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.

Безопасность устройств

Что такое вредоносный код. Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

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.

Методы защиты от вредоносных программ. Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

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.

Безопасность информации

Социальная инженерия: распознать и избежать. Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Ложная информация в Интернете. Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Безопасность при использовании платежных карт в Интернете. Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Беспроводная технология связи. Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Резервное копирование данных. Безопасность личной информации. Создание резервных копий на различных устройствах.

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.

Формой организации внеурочной деятельности является кружок.

Основные виды деятельности:

Конференции, диспуты, конкурсы.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№	Тема	Всего часов	Использование оборудования в центре цифрового и гуманитарного образования «Точка Роста»
<u>Безопасность общения</u>			
1.	Общение в социальных сетях и мессенджерах	1	Ноутбук
2.	С кем безопасно общаться в Интернете	1	Ноутбук
3.	Пароли для аккаунтов социальных сетей	1	Ноутбук
4.	Безопасный вход в аккаунты	1	Ноутбук
5.	Настройки конфиденциальности в социальных сетях	1	Ноутбук
6.	Публикация информации в социальных сетях	1	Ноутбук
7.	Кибербуллинг	1	Ноутбук
8.	Публичные аккаунты	1	Ноутбук
9.	Фишинг	2	Ноутбук
10.	Выполнение и защита индивидуальных и групповых проектов	3	Ноутбук
	Итого:	13	
<u>Безопасность устройств</u>			
11.	Что такое вредоносный код	1	Ноутбук
12.	Распространение вредоносного кода	1	Ноутбук
13.	Методы защиты от вредоносных программ	2	Ноутбук
14.	Распространение вредоносного кода для мобильных устройств	1	Ноутбук
15.	Выполнение и защита индивидуальных и групповых проектов	3	Ноутбук
	Итого:	8	
<u>Безопасность информации</u>			
16.	Социальная инженерия: распознать и избежать	1	Ноутбук

17.	Ложная информация в Интернете	1	Ноутбук
18.	Безопасность при использовании платежных карт в Интернете	1	Ноутбук
19.	Беспроводная технология связи	1	Ноутбук
20.	Резервное копирование данных	1	Ноутбук
21.	Основы государственной политики в области формирования культуры информационной безопасности	2	Ноутбук
22.	Выполнение и защита индивидуальных и групповых проектов	3	Ноутбук
23.	Повторение	3	Ноутбук
	Итого:	13	
	Итого по всем разделам:	34	