

государственное бюджетное общеобразовательное учреждение
Самарской области средняя общеобразовательная школа с. Пискалы
муниципального района Ставропольский Самарской области
(ГБОУ СОШ с. Пискалы)

РАССМОТРЕНО
на заседании методического
объединения учителей
гуманитарного и естественно –
математического циклов.
Руководитель МО
Основа Е.А. Основа

Протокол от 28.08.2019 № 1

СОГЛАСОВАНО.
Заместитель директора по учебно-
воспитательной работе

Горевы Н.Б. Горева
29.08.2019

УТВЕРЖДАЮ.
Директор ГБОУ СОШ с. Пискалы

Гаврилова О.В. Гаврилова
30.08.2019



РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
(общеинтеллектуальное направление развития личности)

7 - 9 классы

Учителя - разработчики:
Кудряшова Ю.В.,
Ятманова Н.А.,
Говоренко Г.В.

Рабочая программа внеурочной деятельности общеинтеллектуального направления «Информационная безопасность» составлена на основе ООП ООО ГБОУ СОШ с. Пискалы.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ

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, со-здание 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 УЧЕБНОГО КУРСА

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.

Формы внеурочной деятельности по направлениям:

Общеинтеллектуальные:

- Предметные недели;
- Конкурсы, экскурсии, олимпиады, конференции, деловые и ролевые;
- Проектная деятельность;
- Участие в научно-исследовательских конференциях;
- Разработка проектов к урокам.

Виды внеурочной деятельности:

1. Словесно-логические.

Основным средством воздействия является слово (убеждение словом), вызывающее ответные эмоции у детей.

- Беседы на различные темы
 - Дискуссии
 - Собрания
 - Конференции
 - Лекции
- #### **2. Игровые (досуговые) формы работы**
- Совместные праздники
 - Подготовка концертов, спектаклей
 - Неделя театра, танца, вокала
 - Просмотр и обсуждение фильмов, спектаклей
 - Соревнования
 - Конкурсы
 - КВНы
 - Туристические походы
 - Экскурсионные прогулки в парк
 - Экскурсионные поездки

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

7 класс

Безопасность общения	Общение в социальных сетях и мессенджерах	1
	С кем безопасно общаться в интернете	1
	Пароли для аккаунтов социальных сетей	1
	Безопасный вход в аккаунты	1
	Настройки конфиденциальности в социальных сетях	1
	Публикация информации в социальных сетях	1
	Кибербуллинг	1
	Публичные аккаунты	1
	Фишинг	2
	Выполнение и защита индивидуальных и групповых проектов	3
Безопасность устройств	Что такое вредоносный код	1
	Распространение вредоносного кода	1
	Методы защиты от вредоносных программ	2
	Распространение вредоносного кода для мобильных устройств	1
	Выполнение и защита индивидуальных и групповых проектов	3
Безопасность информации	Социальная инженерия: распознать и избежать	1
	Ложная информация в Интернете	1
	Безопасность при использовании платежных карт в Интернете	1
	Беспроводная технология связи	1
	Резервное копирование данных	1
	Основы государственной политики в области формирования культуры информационной безопасности	2
	Выполнение и защита индивидуальных и групповых проектов	3
	Повторение, волонтерская практика, резерв	3

8 класс

Информация, компьютер и Интернет.	Компьютер - как он появился, как появился Интернет. закрепление.	1
	Практическая работа №1. Поиск информации в сети Интернет.	1
	Почему компьютер нужно беречь.	1
	Где и как искать информацию для урока.	1
	Где и как искать информацию для урока. Практическое занятие.	1
	Практическая работа №2. Работа с мобильными устройствами (2 ГИС, Госуслуги, Википедия, эл.книги, фотоколлаж, Компас, диктофон, Калькулятор и пр.).	1
	Практическая работа №3. Общение с использованием видеосвязи на примере Skype.	1
	Интернет.	1
	Практическая работа №4. Создание электронной почты.	1
	Проведение текущей аттестации.	1

Техника безопасности и экология.	Гигиена при работе с компьютером. Правила работы с ПК, электронными книгами и мобильными устройствами.	1
	. Сколько времени можно проводить за компьютером. Как правильно сидеть за компьютером.	1
	Как мобильные устройства помогают ориентироваться на местности.	1
	Практическая работа №1. Использование мобильного приложения Компас .	1
	Польза и вред компьютерных игр.	1
	Что делать с компьютером в чрезвычайных ситуациях.	1
	Практическая работа №2. Создание буклетов по темам: • «Как может помочь компьютер в сложных чрезвычайных ситуациях» • «Правила поведения на улице с мобильными устройствами» • «Компьютеру тоже нужна забота» (как ухаживать за ПК и мобильными устройствами)	1
	Улица и мобильные устройства. Компьютер (мобильные устройства) в грозу.	1
Мир виртуальный и реальный. Интернет зависимость.	Что такое Интернет-сообщество.	1
	Социальные сети. Детские социальные сети.	1
	Практическая работа №1. Создание сообщества класса в детских социальных сетях.	1
	Виртуальная личность - что это такое.	1
	Практическая работа №2. Тест «Есть у меня игровая зависимость». Квест «Я умею говорить «Нет» в сети интернет»	1
Методы безопасной работы в Интернете.	Ищите в Интернете только то, что вам требует Как защититься от вредного контента.	1
	Знаки Интернета, рассказывающие об опасной информации.	1
	Признаки работы вирусов. Вирусы и антивирусы.	1
	Что такое электронные деньги, как с ними правильно обращаться.	1
	Практическая работа №1. Исследовательская работа «Колобанга в поисках вируса» (выявление признаков заражения вирусом).	1
Потребительские опасности в Интернете	Интернет и экономика - польза и опасность.	1
	Что такое личная информация.	1
	Практическая работа №1. Прохождение интерактивного курса. «Мошеннические действия в Интернете. Киберпреступления».	1

	Практическая работа №2. Квест «Покупка в интернет-магазине».	1
Основные правила поведения сетевого взаимодействия.	Что такое интернет-этикет.	1
	Практическая работа №1. «Пишу письмо другу».	1
Государственная политика в области защиты информации.	Как государство защищает киберпространство.	1
	Практическая работа №1 Квест «Война миров».	1

9 класс

Информация и личность	Информация. Источники информации. Виды информационных воздействий	1
	Информационная безопасность. Угрозы информационной безопасности.	1
	Передача информации в условиях вынужденного автономного существования	1
	Роль информации в обеспечении личной безопасности.	1
	Уровни и меры защиты информации. Защиты персональной информации	1
	Информация и права потребителя	1
Информация и здоровье	Влияние информации на здоровье человека	1
	Оценка информационных влияний (мотив, цель, средства, реальные результаты). Дезинформация. Реклама.	1
	Оценка информационных влияний (мотив, цель, средства, реальные результаты). Дезинформация. Реклама.2	1
	Оценка информационных влияний (мотив, цель, средства, реальные результаты). Дезинформация. Реклама.3	1
	Методы и средства защиты человека от негативного воздействия информации	1
	Методы и средства защиты человека от негативного воздействия информации2	1
Информация и компьютер	Виды угроз для цифровой информации	1
	Программно-технические меры обеспечения информационной безопасности (параметры безопасности, управление доступом)	1
	Программно-технические меры обеспечения информационной безопасности (антивирусные программы)	1
	Виды программного обеспечения (лицензионное, условно бесплатное, свободно распространяемое). Условия использования	1
Информация и общество	Роль информации в социальных отношениях	1
	Негативные проявления массовой культуры	1

	Информационная безопасность и СМИ. Влияние образной информации на человека	1
	Информационная война	1
	Информационный терроризм	1
Информационная безопасность в сети	Виды и особенности сетевых информационных угроз	1
	Необходимость различных форм контроля над информационными потоками.	1
	Программные средства родительского контроля	1
	Обеспечение информационной безопасности обучающихся. Системы контентной фильтрации.	1
Правовые основы обеспечения информационной безопасности	Свобода доступа к информации и свобода ее распространения	1
	Защита интеллектуальной собственности. Авторское право и тиражирование	1
	Криптография и защита информации. ЭЦП и сертификаты	1
	Правовое регулирование в информационной сфере	1
	Информационная безопасность как составляющая национальной безопасности	1
	Разработка и защита проекта	Разработка и защита проекта1
	Разработка и защита проекта2	1
	Разработка и защита проекта3	1
	Разработка и защита проекта4	1