Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа «Образовательный центр» п.г.т. Рощинский муниципального района Волжский Самарской области

443539, Самарская область, Волжский район, п. г. т. Рощинский, школа.
Официальный сайт учреждения: http://roshchaschool.minobr63.ru
Контактная информация: телефоны: 932 – 82 – 58 (ф), 932 – 82 – 50, адрес электронной почты: roshinsky_sch_vlg@samara.edu.ru

«УТВЕРЖДАЮ»
Приказ от 02.09.2019 г. № 280 - од
Директор школы О. И. Рубина

«ПРОВЕРЕНО»
Заместитель директора по УВР:
Н. С. Дидковская

«РАССМОТРЕНО»
На заседании МО учителей
математики и информатики
Протокол № 1 от 27.08.2019 г.
Руководитель МО А.Ю. Огурцова

C=RU, O="ГБОУ СОШ ""ОЦ"" п.г.т. Рощинский",
CN=Рубина О.И., E=roshinsky_sch_vlg@samara.edu.ru
00ea17aca4d591c1ca
2021.05.11 12:40:40+04'00'

РАБОЧАЯ ПРОГРАММА
курса «Информационная безопасность»/ «Цифровая гигиена»
для 8 (9) класса
ФГОС ООО

Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа «Образовательный центр» п.г.т. Рощинский муниципального района Волжский Самарской области

443539, Самарская область, Волжский район, п. г. т. Рощинский, школа.

Официальный сайт учреждения: http://roshchaschool.minobr63.ru

Контактная информация: телефоны: 932 – 82 – 58 (ф), 932 – 82 – 50, адрес электронной почты: roshinsky_sch_vlg@samara.edu.ru

Для документов

«УТВЕРЖДЕНО»
Приказ от 02.09.2019 г. № 280 - од
Директор школы О. И. Рубина

«ПРОВЕРЕНО»
Заместитель директора по УВР:
Н. С. Дидковская

«РАССМОТРЕНО»
На заседании МО учителей
математики и информатики
Протокол № 1 от 27.08.2019 г.
Руководитель МО А.Ю. Огурцова

РАБОЧАЯ ПРОГРАММА
курса «Информационная безопасность»/ «Цифровая гигиена»
для 8 (9) класса
ФГОС ООО

Аннотация к рабочей программе курса (внеурочной деятельности) «Информационная безопасность»
для 8 (9) класса

Документы, на основе которых составлена рабочая программа	Аннотация
1. Федеральный государственный образовательный стандарт основного общего образования; *2. Основная образовательная программа основного общего образования ГБОУ СОШ «ОЦ» п. г. т. Рощинский* *3.* ***Примерная рабочая программа учебного курса «Цифровая гигиена»,*** *Рекомендованная Координационным советом учебно-методическим объединением в системе общего образования Самарской области (протокол № 27 от 21.08.2019)* *4. ПОЛОЖЕНИЕ о формах, периодичности и порядке текущего контроля успеваемости и промежуточной аттестации обучающихся государственного бюджетного общеобразовательного учреждения Самарской области средней общеобразовательной школы «Образовательный центр» п.г.т. Рощинский муниципального района Волжский Самарской области* *5 ПОЛОЖЕНИЕ о рабочей программе по учебному предмету, курсу, модулю и тематическому (поурочному) планированию в государственном бюджетном общеобразовательном учреждении Самарской области средней общеобразовательной школе «Образовательный центр» п.г.т. Рощинский муниципального района Волжский Самарской области*	Рабочая программа курса «Информационная безопасность» для основной школы предназначена для учащихся 8 (9) классов. В данной программе учитываются доминирующие идеи и положения Программы развития и формирования универсальных учебных действий для основного общего образования, которые обеспечивают формирование российской гражданской идентичности, коммуникативных качеств личности, и способствуют формированию УУД. - *Рабочая программа курса «*Информационная безопасность*» реализуется в учебниках:* - *Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. - М.: Просвещение, 2019. - 80 с.* *- В данной программе учитываются доминирующие идеи и положения Программы развития и формирования универсальных учебных действий для среднего общего образования, которые обеспечивают формирование российской гражданской идентичности, коммуникативных качеств личности, и способствуют формированию УУД.*

I. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА «Информационная безопасность»
В 8 (9) КЛАССЕ

ОБУЧАЮЩИЙСЯ НАУЧИТСЯ	ОБУЧАЮЩИЙСЯ ПОЛУЧИТ ВОЗМОЖНОСТЬ НАУЧИТЬСЯ
ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ:	
- 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,	- основам соблюдения норм информационной этики и права; - основам 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

- приемам безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.	безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

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.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

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

2. 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.

3. 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.

II. СОДЕРЖАНИЕ КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Раздел 1. «Техника безопасности»

Тема 1. Техника безопасности и охрана труда для обучающихся в кабинете информатики и медиатеке. 1 час.

Раздел 2. «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]. 3 часа.

Раздел 3. «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 безопасности при установке приложений на мобильные устройства

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Раздел 4 «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 и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Раздел 5: Повторение - 2 ч

Повторение. 2 часа.

III. ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ курса «Информационная безопасность

№ п/п	ИЗУЧАЕМЫЕ ТЕМЫ (РАЗДЕЛЫ)	Количество часов	Виды деятельности
8 (9) класс			
1.	Техника безопасности	**1**	**организация рабочего места**
2.	Безопасность общения	**13**	**безопасное общение и взаимодействие в процессе использования средств информационных и коммуникационных технологий; учитывать позиции других участников деятельности, эффективно разрешать конфликты;**
3.	Безопасность устройств	**8**	**использование средств информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;**
4.	Безопасность информации	**10**	**использование норм информационной этики и права, принципов обеспечения информационной безопасности, базовых принципов организации и функционирования компьютерных сетей.**
5.	Повторение	**2**	**повторение**
Всего за 1 год обучения		**34**	