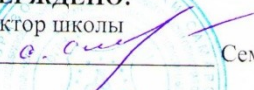


ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ
ОСНОВНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА С. АВЕРЬЯНОВКА
МУНИЦИПАЛЬНОГО РАЙОНА БОГАТОВСКИЙ САМАРСКОЙ ОБЛАСТИ

УТВЕРЖДЕНО:
Директор школы
 Семин С.В.
Приказ № 103/2 от 30.08.2019

РАБОЧАЯ ПРОГРАММА

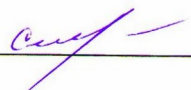
Информационная безопасность
(полное наименование)
6 – 9 классы
(классы)
общее образование
(уровень обучения)
2019 - 2023
(срок реализации)

СОСТАВИТЕЛЬ (РАЗРАБОТЧИК)

Должность: учитель
Ф.И.О. Петрова С.А.
Должность: _____
Ф.И.О. _____

«ПРОВЕРЕНО»

Заместитель директора по УВР:



Семина В.И.

«СОГЛАСОВАНО НА ЗАСЕДАНИИ ШМО»

Рекомендуется к утверждению

Протокол № 1 от 30.08.2019г.

Председатель ШМО:



Уркина П.А.

Дата: 30.08.2019 г.

Планируемые результаты освоения модуля «Информационная безопасность»

Предметные

Выпускник научится	Выпускник овладеет	Выпускник получит возможность овладеть
- 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.	- приемами безопасной организации - своего личного пространства данных с использованием индивидуальных накопителей - данных, интернет-сервисов и т.п.	- 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

Метапредметные

Регулятивные УУД	Познавательные УУД	Коммуникативные УУД
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	- 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,	- 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

существующих возможностей; - выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для	выявлять причины и следствия явлений; - строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим	вывод о достижении цели коммуникации
--	---	---

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.	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.	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;	

Тематическое планирование

№ п / п	Название темы(раздел а)	содержан ие	Кол- во часо в
Раздел 1. «Безопасность общения»			13
1	Общение в социальных сетях и мессенджерах	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	1
2	С кем безопасно общаться в сети Интернет	Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	1
3	Пароли для аккаунтов социальных сетей	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	1
4	Безопасный вход в аккаунты	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	1
5	Настройки конфиденциальности в социальных сетях	Настройки приватности конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	1
6	Публикация	Персональные данные. Публикация	1

	информаци и в социальных сетях	личной информации	
--	---	-------------------	--

7	Кибербуллинг	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	1
8	Публичные аккаунты	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	1
9	Фишинг	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	2
10	Выполнение и защита индивидуальных и групповых проектов		3
Раздел 2. «Безопасность устройств»			7
1	Что такое вредоносный код	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	1
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.	1
3	Методы защиты от вредоносных программ	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	1
4	Распространение вредоносного кода для мобильных устройств.	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	1
5	Выполнение и защита индивидуальных и групповых проектов.		3
Раздел 3 «Безопасность информации»			
1	Социальная инженерия : распознать и	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	1

	избежать		
2	Ложная информация в	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения	1

	Интернете	различных социальных ролей. Фейковые новости. Поддельные страницы.	
3	Безопасность при использовании платежных карт в Интернете	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	1
4	Беспроводная технология связи	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	1
5	Резервное копирование данных	Безопасность личной информации. Создание резервных копий на различных устройствах.	1
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.	2
7	Выполнение и защита индивидуальных и групповых проектов		3
8	Повторение, волонтерская практика, резерв		3
ИТОГО			34