государственное бюджетное общеобразовательное учреждение Самарской области гимназия имени Заслуженного учителя Российской Федерации Сергея Васильевича Байменова города Похвистнево городского округа Похвистнево Самарской области

«Проверено»
Заместитель директора по ВР ГБОУ гимназии
им. С.В.Байменова
города Похвистнево
_____/Н. А. Власова/

30 августа 2019 года

«Утверждаю»
Директор ГБОУ гимназии
им. С.В.Байменова
города Похвистнево
_____/ Т. В. Вагизова/

Приказ № 301-од
от 30 августа 2019 года

РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Наименование курса	**Цифровая гигиена**
Классы	**8А, 8Б, 8В, 9А, 9 Б, 9В**
Количество часов	**34**
Составители	Распанамарева Елена Ивановна
Учителя, работающие по данной программе	

Рассмотрено на заседании методического объединения учителей математики и информатики
протокол № 1
от « 28 » августа 2019 г.
Руководитель МО_____/Волоскова Т.Ю./

2019 - 2020 учебный год

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Огромные массивы информации обрушиваются на человека ежедневно через газеты и журналы, радио и телевидение, всевозможную рекламу.

Психологи все чаще употребляют термин “сжатие миром”. Плотной стеной мир обступает почти каждого из нас, вынуждая воспринимать информацию вне зависимости от возможностей и желания. Порой информация помогает нам ориентироваться в современном мире, а иногда утомляет и мешает принять правильное решение.

Защита человека от поступающей к нему информации является важнейшей составляющей обеспечения его личной безопасности. Человек должен уметь защищаться от возможных информационных манипуляций.

В условиях информатизации общества высокая информационная культура, обеспечивающая информационную безопасность личности, является необходимостью для успешной деятельности в любой сфере.

Теоретически человек сам может переработать любую информацию, но сделает это гораздо эффективнее, если овладеет знаниями и умениями, которыми располагает информационная культура. Поэтому существует острая потребность общества в организации информационного образования, призванного обеспечить формирование информационной культуры и информационной безопасности личности и общества в целом.

Формируя информационную безопасность личности необходимо выработать систему противодействия, защиты личности от возможных информационных манипуляций, а также воспитать чувство ответственности за производство и распространение информации, понимание ее последствий, ее негативного влияния на личность и общество.

Актуальность проблемы воспитания информационной культуры, информационной безопасности обусловлена необходимостью получения знаний, навыков и умений, которыми должен владеть каждый человек в современном, изменяющемся информационном мире. Только личность со сформированной информационной культурой может адекватно реагировать на происходящие в мире процессы. В условиях информатизации общества, всех его структур, высокая информационная культура, обеспечивающая информационную безопасность личности, является необходимостью для успешной деятельности в любой сфере.

Новизна программы состоит в том, что рассматриваются вопросы информационной безопасности, которая является одной из составляющих безопасности личности, а также вопросы информационной культуры личности, которая способствует реальному пониманию человеком самого себя, своего места и роли в окружающем мире.

Элективный курс «Информационная безопасность» разработан для расширения кругозора и формирования мировоззрения учащихся, повышения уровня безопасности человека в окружающей его информационной среде.

Программа предназначена для учащихся 8-9 классов (базовый уровнем знаний, умений и навыков). Объем курса составляет 34 часа (один раз в неделю).

Предложенный материал дополняет образовательные области ОБЖ и информатика, способствует воспитанию информационной культуры обучающихся, формированию информационной безопасности личности, созданию условий для повышения готовности подростков к сознательному, профессиональному и культурному самоопределению в целом.

Цель программы

- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
- формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
- создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
- сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
- сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Формы проведения занятий: беседы, беседы с элементами дискуссий, работа в малых группах, практические работы.

Формы организации деятельности учащихся:

- самостоятельная работа учащихся по практическому использованию различных средств обеспечения информационной деятельности. участие в дискуссиях,

- выработка решения проблем в небольших группах (4-6 человек);
- участие в ролевых ситуациях;
- поисковая деятельность (выявление случаев, проявления негативных или положительных примеров взаимодействия человека и мира информации).

Ожидаемые результаты обучения

После прохождения курса учащиеся должны:

знать:

- понятие и угрозы информационной безопасности,
- уровни защиты информации,
- меры защиты информации,
- правовые акты и нормы по защите информации и авторского права,
- программно-технические меры по защите информации,
- принципы и приемы сетевой безопасности
- уметь:
- использовать возможности ОС WindowsXP для защиты информации;
- применять на практике меры профилактики и защиты информации.

Планируемые результаты освоения обучающимися программы внеурочной деятельности

Личностные универсальные учебные действия

У обучающегося будет формироваться:

- 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.

Познавательные универсальные учебные действия

Обучающийся научится:

- 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.

Регулятивные универсальные учебные действия

Обучающийся научится:

- целеполаганию, включая постановку новых целей, преобразование практической задачи в познавательную;
- самостоятельно анализировать условия достижения цели на основе учета выделенных учителем ориентиров действия в новом учебном материале;
- планировать пути достижения целей;
- уметь самостоятельно контролировать свое время и управлять им.

Коммуникативные универсальные учебные действия

Обучающийся научится:

- 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.

Формы контроля:

1. Рефлексия по каждому занятию в форме вербального проговаривания, письменного выражения своего отношения к теме.
2. По итогам курса обучающиеся выполняют тесты
3. В рамках курса предполагается организовать проектную деятельность учащихся.

Проверка достигаемых учениками образовательных результатов производится в следующих формах:

1. текущий самоанализ, контроль и самооценка учащимися выполняемых заданий;
2. текущая диагностика и оценка учителем деятельности школьников;
3. публичная защита выполненных учащимися творческих работ (индивидуальных и групповых).
4. Каждый раздел учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и проверочного теста.
5. 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.

Тематическое планирование

№	Темы занятий	Кол-во часов	Из них теория	практика
1.	Безопасность общения	14	7	7
2.	Безопасность устройств	12	6	6
3.	Безопасность информации	8	4	4
		34	**17**	**17**

Содержание тем учебного 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 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 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.

Календарно-тематическое планирование

№	Темы занятий	Кол-во часов	Дата
Раздел 1. Безопасность общения - 14 часов			
1.	Общение в социальных сетях и мессенджерах.	1	2.09.19-7.09.19
2.	С кем безопасно общаться в интернете.	1	9.09.19-14.09.19
3.	Пароли для аккаунтов социальных сетей.	1	16.09.19-21.09.19
4.	Безопасный вход в аккаунты.	1	23.09.19-28.09.19
5.	Настройки конфиденциальности в социальных сетях.	1	30.09.19-5.10.19
6.	Публикация информации в социальных сетях.	1	7.10.19-12.10.19
7.	Кибербуллинг.	1	14.10.19-19.10.19
8.	Публичные аккаунты.	1	21.10.19-26.10.19
9-10.	Фишинг.	2	5.11.19-6.11.19
11-14.	Выполнение и защита индивидуальных и групповых проектов.	4	18.11.19-14.12.19
Раздел 2. «Безопасность устройств» -8 часов			
15.	Что такое вредоносный код.	1	16.12.19-21.12.19
16.	Распространение вредоносного кода.	1	23.12.19-28.12.19
17.	Методы защиты от вредоносных программ.	1	13.01.20-18.01.20
18.	Распространение вредоносного кода для мобильных устройств.	1	20.01.20-25.01.20
19-22.	Выполнение и защита индивидуальных и групповых проектов.	4	27.01.20-22.02.20
Раздел 3 «Безопасность информации» - 12 часов			
23.	Социальная инженерия: распознать и избежать.	1	24.02.20-29.02.20
24.	Ложная информация в Интернете.	1	2.03.20-7.03.20
25.	Безопасность при использовании платежных карт в Интернете.	1	9.03.20-14.03.20
26.	Беспроводная технология связи.	1	16.03.20-21.03.20

27.	Основы государственной политики в области формирования культуры информационной безопасности.	1	30.03.20-4.04.20
28-31.	Выполнение и защита индивидуальных и групповых проектов.	4	6.04.20-8.05.20
32-34	Повторение. Волонтерская практика.	3	11.05.20-30.05.20

Учебно-методическое обеспечение программы

Литература:

1. Попов В. Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: Учебное пособие. - М.: Финансы и статистика, 2012.
2. Морозов Н.П., Чернокнижный С.Б. Защита деловой информации для всех. - СПб.: ИД «ВЕСЬ», 2013.
3. Касперский К. Записки исследователя компьютерных вирусов. - СПб.: Питер, 2009.
4. Материалы газеты «Информатика».

Оборудование и приборы:

1. ПК, операционная система Windows или Alt Linux.
2. Пакет офисных приложений MS Office.
3. Ресурсы Единой коллекции цифровых образовательных ресурсов (http://school-collection.edu.ru/).
4. Интернет-ресурсы.

Приложение 1

Требования к содержанию итоговых проектно-исследовательских работ

Критерии содержания текста проектно-исследовательской работы

1. Во введении сформулирована актуальность (личностная и социальная значимость) выбранной проблемы. Тема может быть переформулирована, но при этом четко определена, в необходимости исследования есть аргументы.
2. Правильно составлен научный аппарат работы: точность формулировки проблемы, четкость и конкретность в постановке цели и задач, определении объекта и предмета исследования, выдвижении гипотезы. Гипотеза сформулирована корректно и соответствуют теме работы.
3. Есть планирование проектно-исследовательской деятельности, корректировка ее в зависимости от результатов, получаемых на разных этапах развития проекта. Дана характеристика каждого этапа реализации проекта, сформулированы задачи, которые решаются на каждом этапе, в случае коллективного проекта – распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведен корректно.
4. Используется и осмысляется междисциплинарный подход к исследованию и проектированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников.
5. Определён объём собственных данных и сопоставлено собственное проектное решение с аналоговыми по проблеме. Дан анализ источников и аналогов с точки зрения значимости для собственной проектно-исследовательской работы, выявлена его новизна, библиография и интернет ресурсы грамотно оформлены.
6. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.
7. Есть оценка результативности проекта, соотнесение с поставленными задачами. Проведена оценка социокультурных и образовательных последствий проекта на индивидуальном и общественном уровнях.

Критерии презентации проектно-исследовательской работы (устного выступления)

1. Демонстрация коммуникативных навыков при защите работы. Владение риторическими умениями, раскрытие автором содержание работы, достаточная осведомленность в терминологической системе проблемы, отсутствие стилистических и речевых ошибок, соблюдение регламента.
2. Умение чётко отвечать на вопросы после презентации работы.
3. Умение создать качественную презентацию. Демонстрация умения использовать IT-технологии и создавать слайд презентацию на соответствующем его возрасту уровне.
4. Умение оформлять качественный презентационный буклет на соответствующем его возрасту уровне.
5. Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видеоролик, мультфильм и т.д.).
6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации коммуникабельности, благодарности и уважения по отношению к руководителю, консультантам, умение четко обозначить пути создания сетевого продукта.
7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.