

**муниципальное бюджетное общеобразовательное учреждение
«Гимназия № 133 имени Героя Социалистического Труда М.Б.
Оводенко» городского округа Самара**

«РАССМОТРЕНО»	«ПРОВЕРЕНО»	«УТВЕРЖДАЮ»
на заседании МО	Зам. директора по ВР	Директор
учителей	МБОУ Гимназии №133	МБОУ Гимназии №133
гуманитарного цикла	г.о. Самара	г.о. Самара
Руководитель МО	_____/Обуховой	_____/Терина
_____/Чернышова	Т.Н.	О.Р.
И.Е. протокол № 1	«30» августа 2022г.	Приказ № 352
«30» августа 2022г.		«30» августа 2022г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 009466BAAC1C530512E0EC568B885614E
Владелец: Терина Оксана Радиковна
Действителен: с 19.10.2022 до 12.01.2024

РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности 7 класс

«Информационная безопасность»

Форма организации: общественно-полезные практики

Направление: социальное, «Коммуникативная деятельность»

Срок реализации: 1 год

Разработчик программы:

Учитель информатики
(должность)

Савгильдина И.С.
(Ф.И.О.)

Высшая квалификационная категория

Самара 2022г

Оглавление

У1. ПОЯСНИТЕЛЬНАЯ ЗАПИСЬ

1.1. Актуальность	4
1.2. Практическая значимость.....	4
1.3. Цель внеурочной деятельности.....	4
1.4. Задачи внеурочной деятельности.....	4
1.5. Личностные, метапредметные и предметные результаты внеурочной деятельности «Информационная безопасность».....	8
1.6. Универсальные учебные действия, формируемые в процессе внеурочной деятельности.....	10
2. УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН.....	13
3. СОДЕРЖАНИЕ ПРОГРАММЫ	14
4. МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ.....	16
5. СПИСОК ЛИТЕРАТУРЫ	17

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

При составлении рабочей программы внеурочной деятельности школьников 8 классов «Информационная безопасность» были учтены требования официальных нормативных документов:

- Закон РФ «Об образовании» (в редакции ФЗ от 05.03.2004 г. № 9-ФЗ);
- Приказ Министерства образования и науки РФ от 05.03.2004 г. № 1089 «Об утверждении федерального компонента государственных образовательных стандартов основного общего и среднего (полного) общего образования»;
- Приказ Министерства образования и науки РФ от 09.03.2004 г. № 1312 «Об утверждении федерального базисного учебного плана и примерных учебных планов для общеобразовательных учреждений РФ, реализующих программы общего образования»;
- Приказ Министерства образования и науки РФ от 03.06.2011 г. № 1994 «О внесении изменений в федеральный базисный учебный план и примерные учебные планы для образовательных учреждений Российской Федерации, реализующих программы общего образования, утвержденные приказом Министерства образования и науки Российской Федерации от 9 марта 2004 г. № 1312»;
- Федеральный перечень учебников, рекомендованных (допущенных) Министерством образования к использованию в образовательном процессе в образовательных учреждениях, реализующих образовательные программы общего образования на 2019/2020 учебный год».

1.1. Актуальность

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.

В курсе внеурочной деятельности 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.

Актуальность внеурочной деятельности по информационной безопасности обусловлена также интересом учащихся и запросами их родителей.

1.2. Практическая значимость

В процессе реализации внеурочной деятельности учащиеся познакомятся с основными угрозами безопасности информации, способах защиты информации.

Программа внеурочной деятельности является авторской и разработана на основе учебного пособия «Информационная безопасность, или На расстоянии одного вируса» 7-9 классы: уч. пособие для общеобразоват. организаций/ М.С. Наместникова. – М.: Просвещение, 2019.

1.3. Цель внеурочной деятельности:

Содействие формированию информационной безопасности как неотъемлемой составляющей информационной культуры личности учащегося.

1.4. Задачи внеурочной деятельности:

Обучающие:

- Развитие способности анализировать и оценивать информацию на достоверность;

- Обучение выстраиванию устойчивых алгоритмов поведения в окружающем информационном мире;
- Расширение представления учащихся о правовых и морально-этических нормах в информационной сфере; законодательстве Российской Федерации в области защиты информации и авторского права;
- Обучение способам защиты информации.

Воспитательные:

- Формирование готовности к общению и сотрудничеству со сверстниками и взрослыми в процессе образовательной, общественно-полезной, учебно-исследовательской, творческой деятельности;
- Воспитание целеустремленности в процессе решения учебных задач
- Содействие воспитанию чувства ответственности за производство и распространение информации;
- Воспитание активной жизненной позиции.

Развивающие:

- Развитие самостоятельности, ответственности за результаты своей деятельности.
- Развитие навыков творческой деятельности.

Современное развитие мировой экономики характеризуется все большей зависимостью рынка от значительного объема информационных потоков. Несмотря на все возрастающие усилия по созданию технологий защиты данных, их уязвимость не только уменьшается, но и постоянно возрастает. Поэтому актуальность проблем, связанных с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи, все более усиливается. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важнейших задач. Например, конфиденциальность данных, которая обеспечивается применением различных криптографических методов и средств (шифрование закрывает данные от посторонних лиц, а также решает задачу их целостности); идентификация пользователя на основе анализа кодов, используемых им для подтверждения своих прав на доступ в систему (сеть), на работу с данными и на их изменение, и т.д. Интенсивное развитие современных информационных технологий, и в особенности сетевых технологий, для этого создает все предпосылки. В настоящее время значительно расширились функциональные возможности и повысился «интеллект»

средств обработки и передачи данных, а также технических средств, применяемых для защиты информации.

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

В соответствии со «Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года», утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, «Стратегией развития информационного общества в Российской Федерации», утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 и рядом других документов в числе многих других задач выделяются:

- обеспечение различных сфер экономики качественными информационными технологиями;
- обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Безопасность в информационном обществе является одним из основных направлений фундаментальных исследований в области информационных технологий.

Компьютерные технологии применяются при изучении практически всех школьных дисциплин уже с младших классов, поэтому, как указано в «Стратегии развития отрасли информационных технологий в Российской Федерации»: «Необходимо совершенствовать современную профессиональную подготовку учителей информатики и преподавателей дисциплин в сфере информационных технологий», а значит, и в сфере кибербезопасности. Киберугрозы существуют везде, где применяются информационные технологии, следовательно, преподаватель любой дисциплины может в профессиональной деятельности столкнуться и со спамом, и с вирусами, и со взломом компьютера и с многими другими проблемами, на которые нужно не только оперативно

реагировать, но и насколько возможно уметь предотвращать их появление, а значит, постоянно упоминать в контексте урока различные аспекты организации информационной безопасности. Преподаватель должен иметь представление о современном уровне развития вычислительной техники, информационных сетей, технологий коммуникации и навигации.

Государство считает необходимым расширение объема преподавания информационных технологий в общеобразовательных организациях. В качестве одной из организационных мер в обеспечении кибербезопасности определена разработка и внедрение в учебный процесс образовательных организаций разного уровня курса по информационной безопасности.

С учетом роста числа угроз информационной деятельности и стремительного развития информационных технологий представляется необходимым включить в ФГОСы соответствующие требования, что позволило бы органически дополнить образовательный процесс новыми модулями без рассогласования с имеющимися учебными планами. В число требований к результатам подготовки учащихся необходимо включить не только «удовлетворение познавательных интересов, поиск дополнительной информации», знание «технических устройств (в том числе компьютеров)», умение «искать информацию с применением правил поиска (построения запросов) в базах данных, компьютерных сетях, пользоваться персональным компьютером и его периферийным оборудованием; следовать требованиям техники безопасности, гигиены, эргономики и ресурсосбережения при работе со средствами информационных и коммуникационных технологий», но и знание основ кибербезопасности, умения соблюдать требования кибербезопасности в практической деятельности и организовывать безопасность личного информационного пространства.

Необходимо отметить, что в настоящее время в рамках метапредметных результатов и предметных умений дисциплины «Информатика» вопросы информационной безопасности обозначены:

- требование формирования навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права;
- умения использовать средства 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;

- понимание основ правовых аспектов использования компьютерных программ и работы в Интернете и т.п.

На проведение внеурочной деятельности по информатике «Информационная безопасность» в 8-ых классах отводится по 1 часу в неделю, всего 34 часа. На занятиях предусмотрено проведение большого количества практических работ и выполнение проекта.

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.

1.5. Личностные, метапредметные и предметные результаты внеурочной деятельности «Информационная безопасность»

Метапредметные результаты:

- умение самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учебе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности;
- владение основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности;
- умение определять понятия, создавать обобщения, устанавливать аналогии, классифицировать, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно-следственные связи, строить логическое рассуждение, умозаключение (индуктивное, дедуктивное и по аналогии) и делать выводы;
- умение создавать, применять и преобразовывать знаки и символы, модели и схемы для решения учебных и познавательных задач;
- смысловое чтение;
- умение осознанно использовать речевые средства в соответствии с задачей коммуникации; владение устной и письменной речью;
- формирование и развитие компетентности в области использования информационно-коммуникационных технологий (далее ИКТ-компетенции).

Предметные результаты:

- применять антивирусные программы для обеспечения стабильной работы технических средств ИКТ;

- понимать основные принципы устройства современного компьютера и мобильных электронных устройств; использовать правила безопасной и экономичной работы с компьютерами и мобильными устройствами;
- критически оценивать информацию, полученную из сети Интернет;
- кодировать и декодировать тексты по заданной кодовой таблице; строить неравномерные коды, допускающие однозначное декодирование сообщений; понимать задачи построения кода, обеспечивающего по возможности меньшую среднюю длину сообщения при известной частоте символов, и кода, допускающего диагностику ошибок;
- применять на практике принципы обеспечения информационной безопасности, способы и средства обеспечения надежного функционирования средств ИКТ; соблюдать при работе в сети нормы информационной этики и права (в том числе авторские права);
- следовать основам безопасной и экономичной работы с компьютерами и мобильными устройствами; соблюдать санитарно-гигиенические требования при работе за персональным компьютером в соответствии с нормами действующих СанПиН.

Личностные результаты:

- способность увязать учебное содержание с собственным жизненным опытом, понять значимость подготовки в области информатики в условиях развития информационного общества;
- готовность к повышению своего образовательного уровня и продолжению обучения с использованием средств и методов информатики;
- способность и готовность к общению и сотрудничеству со сверстниками и взрослыми в процессе образовательной, общественно-полезной, учебно-исследовательской, творческой деятельности;
- способность и готовность к принятию ценностей здорового образа жизни за счет знания основных гигиенических, эргономических и технических условий безопасной эксплуатации средств ИКТ.

1.6. Универсальные учебные действия, формируемые в процессе внеурочной деятельности.

1. *Личностные универсальные учебные действия* обеспечивают ценностно-смысловую ориентацию учащихся и ориентацию в социальных ролях и межличностных отношениях. К ним относятся:
 - a. действие смыслообразования, т. е. установление учащимися связи между целью учебной деятельности (результатом учения) и ее мотивом (тем, что побуждает деятельность, ради чего она осуществляется); ученик должен задаваться вопросом о том, «какое значение, смысл имеет для меня учение», и уметь находить ответ на него;
 - b. действие нравственно-этического оценивания усваиваемого содержания, исходя из социальных и личностных ценностей, обеспечивающее личностный моральный выбор.

2. *Регулятивные универсальные учебные действия* обеспечивают организацию учащимся своей учебной деятельности; к ним относятся:
 - a. целеполагание как постановка учебной задачи на основе соотнесения того, что уже известно и усвоено учащимся, и того, что еще неизвестно;
 - b. планирование — определение последовательности промежуточных целей с учетом конечного результата; составление плана и последовательности действий;
 - c. прогнозирование — предвосхищение результата и уровня усвоения, его временных характеристик;
 - d. контроль в форме сличения способа действия и его результата с заданным эталоном с целью обнаружения отклонений и отличий от эталона;
 - e. коррекция — внесение необходимых дополнений и корректив в план и способ действия в случае расхождения эталона, реального действия и его продукта;
 - f. оценка — выделение и осознание учащимся того, что уже усвоено и что еще подлежит усвоению, осознание качества и уровня усвоения;
 - g. волевая саморегуляция как способность к мобилизации сил и энергии; способность к волевому усилию — к выбору в ситуации мотивационного конфликта и к преодолению препятствий.

3. *Познавательные универсальные учебные действия* включают действия исследования, поиска и отбора необходимой информации, ее структурирования; моделирования изучаемого содержания; логические действия и операции; способы решения задач. Познавательные УУД разделяются на группы:
- а. *общеучебные универсальные действия*:
 - самостоятельное выделение и формулирование познавательной цели;
 - структурирование знаний;
 - умение адекватно, осознанно и произвольно строить речевое высказывание в устной и письменной речи;
 - действие со знаково-символическими средствами и моделирование;
 - смысловое чтение как осмысление цели чтения и выбор вида чтения в зависимости от цели;
 - б. *логические действия*:
 - выбор оснований, критериев для сравнения, оценки и классификации объектов;
 - синтез как составление целого из частей;
 - подведение под понятия, распознавание объектов;
 - выявление родо-видовых и ситуативно существенных признаков;
 - выдвижение гипотез и их доказательство;
 - с. *действия постановки и решения проблемы*:
 - формулирование проблемы;
 - самостоятельное создание алгоритмов деятельности при решении проблем творческого и поискового характера.
4. *Коммуникативные универсальные учебные действия* обеспечивают социальную компетентность и сознательную ориентацию учащихся на позиции других людей (прежде всего, партнера по общению или деятельности), умение слушать и вступать в диалог, участвовать в коллективном обсуждении проблем, интегрироваться в группу сверстников и строить продуктивное взаимодействие и сотрудничество со сверстниками и взрослыми.

Для проверки знаний и умений учащихся осуществляется как текущий, так и итоговый контроль. Текущий контроль уровня усвоения материала осуществляется по результатам выполнения учащимися практикума по каждой теме внеурочной деятельности. Итоговый контроль реализуется в форме проекта.

Предметом диагностики и контроля являются внешние образовательные продукты учеников, а также их внутренние личностные качества (освоенные способы деятельности, знания, умения), которые относятся к целям и задачам курса.

Основой для оценивания деятельности учеников являются результаты анализа его продукции и деятельности по ее созданию. Оценка имеет различные способы выражения — устные суждения педагога, письменные качественные характеристики, систематизированные по заданным параметрам аналитические данные, в том числе и рейтинги.

Ученик выступает полноправным субъектом оценивания. Одна из задач педагога — обучение детей навыкам самооценки. С этой целью учитель выделяет и поясняет критерии оценки, учит детей формулировать эти критерии в зависимости от поставленных целей и особенностей образовательного продукта — программы и творческого проекта

Проверка достигаемых учениками образовательных результатов производится в следующих формах:

- 1) текущий рефлексивный самоанализ, контроль и самооценка учащимися выполняемых заданий;
- 2) взаимооценка учащимися работ друг друга или работ, выполненных в группах;
- 3) текущая диагностика и оценка учителем деятельности школьников;
- 4) итоговая оценка деятельности и образовательной продукции ученика в соответствии с его индивидуальной образовательной программой;
- б) итоговая оценка индивидуальной деятельности учащихся учителем, выполняемая в форме образовательной характеристики.

Выполненные учащимися работы включаются в их «портфель достижений».

Итоговый контроль проводится в конце всего курса. Он может иметь форму зачета или защиты творческих работ. Данный тип контроля предполагает комплексную проверку образовательных результатов по всем заявленным целям и направлениям курса.

2. УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование тем	Кол-во часов в программе (теория, практика)
1	Общие проблемы безопасности Национальные интересы и безопасность Информационная безопасность, информационная война	2
2	Безопасность общения Общение в социальных сетях и мессенджерах С кем безопасно общаться в Интернете Пароли для аккаунтов социальных сетей Вход в аккаунт социальных сетей Настройка конфиденциальности в социальных сетях и мессенджерах Кибербуллинг Публичные аккаунты Фишинг Обобщение по темам раздела	9 (на каждом занятии 20 минут - теория, 20 минут – практическая работа)
3	Безопасность устройств Что такое вредоносный код Распространение вредоносного кода Методы защиты от вредоносных программ Распространение вредоносного кода для мобильных устройств Обобщение по темам раздела	5 (на каждом занятии 20 минут - теория, 20 минут – практическая работа)
4	Безопасность информации Социальная инженерия: распознать и избежать Ложная информация в Интернете Безопасность при использовании платёжных карт в Интернете Беспроводная технология связи Резервное копирование данных Обобщение по темам раздела	6 (на каждом занятии 20 минут - теория, 20 минут – практическая работа)
5	Криптография и криптоанализ Методы криптографического преобразования данных Шифрование заменой Монофоническая замена Шифрование методом перестановок Обобщение по темам раздела	8 (на каждом занятии 20 минут - теория, 20 минут – практическая работа)
6	Работа над проектом Защита проекта	4

3. СОДЕРЖАНИЕ ПРОГРАММЫ

№ блока	Название и содержание блока	Кол-во часов по теме	Формы контроля
Общие проблемы безопасности			
1	Национальные интересы и безопасность	1	
2	Информационная безопасность, информационная война	1	
Безопасность общения			
3	Общение в социальных сетях и мессенджерах	1	Практические работы
4	С кем безопасно общаться в Интернете	1	
5	Пароли для аккаунтов социальных сетей	1	
6	Вход в аккаунт социальных сетей	1	
7	Настройка конфиденциальности в социальных сетях и мессенджерах	1	
8	Кибербуллинг	1	
9	Публичные аккаунты	1	
10	Фишинг	1	
11	Обобщение по темам раздела	1	
Безопасность устройств			
12	Что такое вредоносный код	1	Практические работы
13	Распространение вредоносного кода	1	
14	Методы защиты от вредоносных программ	1	
15	Распространение вредоносного кода для мобильных устройств	1	
16	Обобщение по темам раздела	1	
Безопасность информации			
17	Социальная инженерия: распознать и избежать	1	Практические работы
18	Ложная информация в Интернете	1	

19	Безопасность при использовании платёжных карт в Интернете	1	
20	Беспроводная технология связи	1	
21	Резервное копирование данных	1	
22	Обобщение по темам раздела	1	
Криптография и криптоанализ			
23	Методы криптографического преобразования данных	1	Практические работы
24	Шифрование заменой	2	
25	Монофоническая замена	2	
26	Шифрование методом перестановок	2	
27	Обобщение по темам раздела	1	
	Работа над проектом	3	
	Защита проекта	1	

4. МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

В процессе реализации внеурочной деятельности учащихся 8 классов основной школы «Информационная безопасность» предусмотрены индивидуальная, фронтальная и групповая формы работы учащихся.

Помещение кабинета информатики, его оборудование (мебель и средства ИКТ) должны удовлетворять требованиям действующих Санитарно-эпидемиологических правил и нормативов (СанПиН 2.4.2.2821-10, СанПиН 2.2.2/2.4.1340-03).

В кабинете информатики должны быть оборудованы не менее одного рабочего места преподавателя и 12–15 рабочих мест учащихся, снабженных стандартным комплектом: системный блок, монитор, устройства ввода текстовой информации и манипулирования экранными объектами (клавиатура и мышь), привод для чтения и записи компакт-дисков, аудио/видео входы/выходы.

Компьютерное оборудование может быть представлено как в стационарном исполнении, так и в виде переносных компьютеров.

Кабинет информатики комплектуется следующим периферийным оборудованием:

- принтер (черно-белой печати, формата А4);
- мультимедийный проектор (рекомендуется консольное крепление над экраном или потолочное крепление), подсоединяемый к компьютеру преподавателя;
- экран (на штативе или настенный) или интерактивная доска.

Компьютерное оборудование может использовать операционные системы Windows или Linux.1. Все программные средства, устанавливаемые на компьютерах в кабинете информатики, должны быть лицензированы для использования на необходимом числе рабочих мест.

5. СПИСОК ЛИТЕРАТУРЫ

1. Федеральный государственный образовательный стандарт основного общего образования <http://минобрнауки.рф/документы/938>
2. «Информационная безопасность, или На расстоянии одного вируса» 7-9 классы: уч. пособие для общеобразоват. организаций/ М.С. Наместникова. – М.: Просвещение, 2019
3. Партыка Т.Л., Попов И.И. «Информационная безопасность» М., Форум, 2010.