МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Министерство образования Архангельской области

Управление образования Администрации Северодвинска

МАОУ "СОШ №19"

Яркова Елена Валентиновна

Подписано цифровой подписью: Яркова Елена Валентиновна
Дата: 2023.10.22 16:19:09 +03'00'

СОГЛАСОВАНО	УТВЕРЖДЕНО
Заместитель директора	Директор МАОУ
по ВР	"СОШ № 19"
_____	_____
Жиганова В.В.	Яркова Е.В.
«31» августа 2023 г.	«31» августа 2023 г.

РАБОЧАЯ ПРОГРАММА

Курса внеурочной деятельности

«Информационная безопасность»

для обучающихся 9 классов

Северодвинск 2023

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа курса внеурочной деятельности «Информационная безопасность, или На расстоянии одного вируса» адресована учащимся 9 классов и направлена на достижение следующих планируемых результатов Федерального государственного образовательного стандарта основного общего образования: предметных (образовательные области «Математика и информатика», «Физическая культура, экология и ОБЖ»); метапредметных (регулятивных, познавательных, коммуникативных); личностных.

Курс является важной составляющей частью работы с учащимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.), задумывающимися о своей личной безопасности, безопасности своей семьи и своих друзей, а также проявляющими интерес к изучению истории и технологических основ информационной безопасности.

Направление программы курса внеурочной деятельности – общекультурное. Программа курса ориентирована на выполнение требований к организации и содержанию внеурочной деятельности школьников. Ее реализация даёт возможность раскрытия индивидуальных способностей школьников, развития интереса к различным видам индивидуальной и групповой деятельности, закрепления умения самостоятельно организовать свою учебную, в том числе проектную деятельность. Кроме того, программа курса дает возможность закрепить ряд результатов обучения, предусмотренных программами учебных курсов по предметам «Информатика» и «Основы безопасности жизнедеятельности».

Цель программы:

- формирование активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им;
- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз.

Задачи программы:

- дать представление о современном информационном обществе, информационной безопасности личности и государства;

- сформировать навыки ответственного и безопасного поведения в современной информационно-телекоммуникационной среде;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом;
- сформировать общекультурные навыки работы с информацией (умений грамотно пользоваться источниками информации, правильно организовать информационный процесс);
- дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;
- познакомить со способами защиты от противоправных посягательств в сети Интернет, защиты личных данных.

Учет рабочей программы воспитания МАОУ «СОШ №19» реализуется через воспитательный потенциал курса «Информационная безопасность»:

- установление доверительных отношений между педагогическим работником и обучающимися, способствующих позитивному восприятию обучающимися требований и просьб педагогического работника, привлечению их внимания к обсуждаемой на уроке информации, активизации познавательной деятельности;
- побуждение обучающихся соблюдать на уроке общепринятые нормы поведения, правила общения со старшими и сверстниками, принципы учебной дисциплины и самоорганизации;
- знать роль инженерной графики в современном мире для осознания положительного и отрицательного воздействия её на общество;
- формирование патриотического воспитания, понимать роль отечественных ученых в становлении инженерных наук;
- формирование устойчивого познавательного интереса, любознательности в изучении инженерной графики путём получения дополнительной информации из различных источников.
- включение в урок игровых процедур, которые помогают поддержать мотивацию обучающихся к получению знаний, налаживанию позитивных межличностных отношений в классе, помогают установлению доброжелательной атмосферы во время урока.

Курс внеурочной деятельности «Информационная безопасность» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей.

Программа учебного курса «Информационная безопасность» рассчитана на 34 учебных часа в 9 классах.

СОДЕРЖАНИЕ КУРСА

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Система учебных заданий, предложенная в учебном курсе, позволяет создать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им, и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз.

Система заданий предполагает индивидуальную и групповую формы работы, составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы. Предлагаемые задания направлены на формирование критичного мышления школьников, формирование умений решать проблемы, работать в команде, высказывать и защищать собственную позицию, приобретение основ безопасной работы с информацией в виртуальном мире. В учебном пособии предложены следующие виды заданий: задания для подготовки устного ответа; задания, выполняемые с помощью интернета; задания, выполняемые на заранее учителем подготовленных листах. Готовые листы для последнего вида задания учитель имеет возможность распечатать со страницы сайта издательства «Просвещение», расположенной по адресу https://catalog.prosv.ru/item/36980.

Каждый раздел программы завершается выполнением проверочного теста и проектной работой по одной из тем, предложенных на выбор учащихся.

За счет часов, предусмотренных для повторения материала (2 часа), возможно проведение учебных занятий/классных часов 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, подготовленные в ходе выполнения заданий по темам пособия. Программа учебного курса рассчитана на 34 учебных часа, из них 27 часов - учебных занятий, 3 часа - проверка знаний, 4 часа - подготовка и защита учебных проектов.

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.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

Личностные результаты отражают готовность и способность обучающихся руководствоваться сформированной внутренней позицией личности, системой ценностных ориентаций, позитивных внутренних убеждений, соответствующих традиционным ценностям российского общества, расширение жизненного опыта и опыта деятельности в процессе реализации средствами учебного предмета основных направлений воспитательной деятельности.

В результате изучения информатики на уровне среднего общего образования у обучающегося будут сформированы следующие личностные результаты:

1) гражданского воспитания:

осознание своих конституционных прав и обязанностей, уважение закона и правопорядка, соблюдение основополагающих норм информационного права и информационной безопасности; готовность противостоять идеологии экстремизма, национализма, ксенофобии, дискриминации по социальным, религиозным, расовым, национальным признакам в виртуальном пространстве;

2) патриотического воспитания:

ценностное отношение к историческому наследию, достижениям России в науке, искусстве, технологиях, понимание значения информатики как науки в жизни современного общества;

3) духовно-нравственного воспитания:

сформированность нравственного сознания, этического поведения; способность оценивать ситуацию и принимать осознанные решения, ориентируясь на морально-нравственные нормы и ценности, в том числе в сети Интернет;

4) эстетического воспитания:

эстетическое отношение к миру, включая эстетику научного и технического творчества; способность воспринимать различные виды искусства, в том числе основанного на использовании информационных технологий;

5) физического воспитания:

сформированность здорового и безопасного образа жизни, ответственного отношения к своему здоровью, в том числе за счёт соблюдения требований безопасной эксплуатации средств информационных и коммуникационных технологий;

6) трудового воспитания:

готовность к активной деятельности технологической и социальной направленности, способность инициировать, планировать и самостоятельно выполнять такую деятельность; интерес к сферам профессиональной деятельности, связанным с информатикой, программированием и информационными технологиями, основанными на достижениях науки информатики и научно-технического прогресса, умение совершать осознанный выбор будущей профессии и реализовывать собственные жизненные планы; готовность и способность к образованию и самообразованию на
протяжении всей жизни;

7) экологического воспитания:

осознание глобального характера экологических проблем и путей их
решения, в том числе с учётом возможностей информационно-коммуникационных технологий;

8) ценности научного познания:

сформированность мировоззрения, соответствующего современному уровню развития науки, достижениям научно-технического прогресса и общественной практики, осознание ценности научной деятельности, готовность осуществлять проектную и исследовательскую деятельность индивидуально и в группе.

В процессе достижения личностных результатов освоения программы по информационной безопасности у обучающихся совершенствуется эмоциональный интеллект, предполагающий сформированность:

саморегулирования, включающего самоконтроль, умение принимать ответственность за своё поведение, способность адаптироваться к эмоциональным изменениям и проявлять гибкость, быть открытым новому; внутренней мотивации, включающей стремление к достижению цели и успеху, оптимизм, инициативность, умение действовать, исходя из своих возможностей; эмпатии, включающей способность понимать эмоциональное состояние других, учитывать его при осуществлении коммуникации, способность к сочувствию и сопереживанию; социальных навыков, включающих способность выстраивать отношения с другими людьми, заботиться, проявлять интерес и разрешать конфликты.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

В результате изучения информационной безопасности у обучающегося будут сформированы метапредметные результаты, отраженные в универсальных учебных действиях, а именно – познавательные универсальные учебные действия, коммуникативные универсальные учебные действия, регулятивные универсальные учебные действия, совместная деятельность.

Познавательные универсальные учебные действия

1) базовые логические действия:

самостоятельно формулировать и актуализировать проблему, рассматривать её всесторонне; устанавливать существенный признак или основания для сравнения, классификации и обобщения; определять цели деятельности, задавать параметры и критерии их достижения; выявлять закономерности и противоречия в рассматриваемых явлениях; разрабатывать план решения проблемы с учётом анализа имеющихся материальных и нематериальных ресурсов; вносить коррективы в деятельность, оценивать соответствие результатов целям, оценивать риски последствий деятельности; координировать и выполнять работу в условиях реального, виртуального и комбинированного взаимодействия; развивать креативное мышление при решении жизненных проблем.

2) базовые исследовательские действия:

владеть навыками учебно-исследовательской и проектной деятельности, навыками разрешения проблем, способностью и готовностью к самостоятельному поиску методов решения практических задач, применению различных методов познания; осуществлять различные виды деятельности по получению нового знания, его интерпретации, преобразованию и применению в различных учебных ситуациях, в том числе при создании учебных и социальных проектов; формировать научный тип мышления, владеть научной терминологией, ключевыми понятиями и методами; ставить и формулировать собственные задачи в образовательной деятельности и жизненных ситуациях;

выявлять причинно-следственные связи и актуализировать задачу, выдвигать гипотезу её решения, находить аргументы для доказательства своих утверждений, задавать параметры и критерии решения; анализировать полученные в ходе решения задачи результаты, критически оценивать их достоверность, прогнозировать изменение в новых условиях; давать оценку новым ситуациям, оценивать приобретённый опыт; осуществлять целенаправленный поиск переноса средств и способов
действия в профессиональную среду; уметь переносить знания в познавательную и практическую области жизнедеятельности; уметь интегрировать знания из разных предметных областей; выдвигать новые идеи, предлагать оригинальные подходы и решения, ставить проблемы и задачи, допускающие альтернативные решения.

3) работа с информацией:

владеть навыками получения информации из источников разных типов, самостоятельно осуществлять поиск, анализ, систематизацию и интерпретацию информации различных видов и форм представления; создавать тексты в различных форматах с учётом назначения информации и целевой аудитории, выбирая оптимальную форму представления и визуализации; оценивать достоверность, легитимность информации, её соответствие
правовым и морально-этическим нормам; 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;

владеть навыками распознавания и защиты информации, информационной безопасности личности.

Коммуникативные универсальные учебные действия

1) общение:

осуществлять коммуникации во всех сферах жизни;

распознавать невербальные средства общения, понимать значение социальных знаков, распознавать предпосылки конфликтных ситуаций и смягчать конфликты; владеть различными способами общения и взаимодействия, аргументированно вести диалог, уметь

смягчать конфликтные ситуации; развёрнуто и логично излагать свою точку зрения с использованием
языковых средств.

2) совместная деятельность:

понимать и использовать преимущества командной и индивидуальной работы; выбирать тематику и методы совместных действий с учётом общих интересов и возможностей каждого члена коллектива; принимать цели совместной деятельности, организовывать и координировать действия по их достижению: составлять план действий, распределять роли с учётом мнений участников, обсуждать результаты совместной работы; оценивать качество своего вклада и каждого участника команды в общий результат по разработанным критериям; предлагать новые проекты, оценивать идеи с позиции новизны, оригинальности, практической значимости; осуществлять позитивное стратегическое поведение в различных ситуациях, проявлять творчество и воображение, быть инициативным.

Регулятивные универсальные учебные действия

1) самоорганизация:

самостоятельно осуществлять познавательную деятельность, выявлять проблемы, ставить и формулировать собственные задачи в образовательной деятельности и жизненных ситуациях; самостоятельно составлять план решения проблемы с учётом имеющихся ресурсов, собственных возможностей и предпочтений; давать оценку новым ситуациям; расширять рамки учебного предмета на основе личных предпочтений; делать осознанный выбор, аргументировать его, брать ответственность за решение; оценивать приобретённый опыт; способствовать формированию и проявлению широкой эрудиции в разных областях знаний, постоянно повышать свой образовательный и культурный уровень.

2) самоконтроль:

давать оценку новым ситуациям, вносить коррективы в деятельность, оценивать соответствие результатов целям; владеть навыками познавательной рефлексии как осознания совершаемых действий и мыслительных процессов, их результатов и оснований, использовать приёмы рефлексии для оценки ситуации, выбора верного

решения; оценивать риски и своевременно принимать решения по их снижению; принимать мотивы и аргументы других при анализе результатов деятельности.

3) принятия себя и других:

принимать себя, понимая свои недостатки и достоинства; принимать мотивы и аргументы других при анализе результатов

деятельности; признавать своё право и право других на ошибку; развивать способность понимать мир с позиции другого человека.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

В процессе изучения внеурочного курса информационной безопасности ***в 9 классе*** обучающимися будут достигнуты следующие 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 приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.,
- основы соблюдения норм информационной этики и права овладеть 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
- в ходе изучения учебного курса, обучающиеся усовершенствуют опыт проектной деятельности и навыки работы с информацией, в том числе в текстовом, табличном виде, виде диаграмм и пр.
- смогут идентифицировать собственные проблемы и определять главную проблему;
- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Наименование разделов и тем программы	Количество часов			Электронные (цифровые) образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
1	Безопасность общения	11	1	10	https://catalog.prosv.ru/item/36980
2	Безопасность устройств	6	1	5	https://catalog.prosv.ru/item/36980
3	Безопасность информации	13	1	12	https://catalog.prosv.ru/item/36980
4	Подготовка и защита учебных проектов	4		4	https://catalog.prosv.ru/item/36980
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	3	31	

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ

№ п/п	Тема урока
1	Общение в социальных сетях и мессенджерах
2	С кем безопасно общаться в интернете
3	Пароли для аккаунтов социальных сетей
4	Безопасный вход в аккаунты
5	Настройки конфиденциальности в социальных сетях
6	Настройки конфиденциальности в социальных сетях
7	Публикация информации в социальных сетях
8	Кибербуллинг
9	Кибербуллинг
10	Публичные аккаунты
11	Публичные аккаунты
12	Фишинг
13	Что такое вредоносный код?
14	Распространение вредоносного кода
15	Распространение вредоносного кода
16	Методы защиты от вредоносных программ

17	Методы защиты от вредоносных программ
18	Распространение вредоносного кода для мобильных устройств
19	Распространение вредоносного кода для мобильных устройств

20	Социальная инженерия: распознать и избежать
21	Социальная инженерия: распознать и избежать
22	Ложная информация в Интернете
23	Безопасность при использовании платежных карт в Интернете
24	Безопасность при использовании платежных карт в Интернете
25	Беспроводная технология связи
26	Беспроводная технология связи
27	Резервное копирование данных
28	Резервное копирование данных
29	Основы государственной политики в области формирования культуры информационной безопасности
30	Основы государственной политики в области формирования культуры информационной безопасности
31	Выполнение и защита индивидуальных и групповых проектов
32	Выполнение и защита индивидуальных и групповых проектов
33	Выполнение и защита индивидуальных и групповых проектов
34	Выполнение и защита индивидуальных и групповых проектов