

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
САМАРСКОЙ ОБЛАСТИ ОСНОВНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 20 ИМЕНИ
В.Ф.ГРУШИНА ГОРОДА НОВОКУЙБЫШЕВСКА ГОРОДСКОГО ОКРУГА НОВОКУЙБЫШЕВСК
САМАРСКОЙ ОБЛАСТИ**

Рассмотрено
на заседании методического
совета
Е.А.Осипова

Проверено
заместитель директора по ВР
Е.Г.Бердникова

Утверждено
приказом от 21.06.2022 № 350-од
директор ГБОУ ООШ № 20
г.Новокуйбышевска
О.И.Беседина

**Рабочая программа внеурочной деятельности
«Информационная безопасность («Цифровая гигиена»)»
7-9 классы**



C=RU, O=ГБОУ ООШ № 20
г.Новокуйбышевска, CN=Беседина О.И.,
E=sch20_nkb@samara.edu.ru
00beb6a220ea759ede
2022.09.01 16:58:06+04'00'

Пояснительная записка

Программа внеурочной деятельности «**Информационная безопасность**» рассчитана на 1 год обучения и предназначена для учащихся 7-9-х классов.

Программа включает три раздела:

- «Результаты освоения курса внеурочной деятельности»;
- «Содержание курса внеурочной деятельности» с указанием форм организации и видов деятельности;
- «Тематическое планирование».

Рабочая программа разработана в соответствии с:

- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями от 07.05.2013 г., 02.07.2013 г.; 23.07.2013 г., 25.11.2013 г., 03.02.2014 г., 05.05.2014 г., 27.05.2014 г., 04.06.2014 г., 28.06.2014 г., 21.07.2014 г., 31.12.2014 г., 06.04.2015 г., 02.05.2015 г., 29.06.2015 г., 13.07.2015 г., 14.12.2015 г., 29.12.2015 г., 30.12.2015 г., 02.03.2016 г., 02.06.2016 г., 03.07.2016 г., 01.05.2017 г., 29.07.2017 г., 29. 12.2017 г.);
- Федеральным государственным образовательным стандартом основного общего образования, утвержденным приказом Министерства образования и науки Российской Федерации от 17 декабря 2010 г. № 1897 (с изменениями и дополнениями от 29.12.2014 г. № 1644; 31.12.2015 г. № 1577);
- Концепцией духовно-нравственного развития и воспитания личности гражданина России / А.Я.Данилюк, А.М. Кондаков, В.А. Тишков. - М. Просвещение, 2014;
- Приказом Минобрнауки Российской Федерации от 04.10.2010г. № 986, г. Москва «Об утверждении федеральных требований к образовательным учреждениям в части минимальной оснащённости учебного процесса и оборудования учебных помещений»;
- СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения, содержания в общеобразовательных организациях» (утвержденные Постановлением Главного государственного санитарного врача Российской Федерации от 24.11.2015 N81 «Об утверждении СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях»);
- Примерной рабочей программой учебного курса «Цифровая гигиена», - Самара, 2019 (Программа модуля «Информационная безопасность» разработана на основе программы курса «Информационная безопасность, или на расстоянии одного вируса» Наместниковой М.С)

- Основной образовательной программой основного общего образования ГБОУ ООШ № 19.

Результаты освоения курса внеурочной деятельности

Функциональная грамотность

Одним из приоритетных планируемых образовательных результатов является формирование *функциональной грамотности* обучающегося. Этот термин отражает общеучебную компетенцию, что на современном этапе обеспечивается за счет внедрения Федерального образовательного стандарта всех ступеней образования. Лишь функционально грамотная личность способна использовать все постоянно приобретаемые в течение жизни знания, умения и навыки для решения максимально широкого диапазона жизненных задач в различных сферах человеческой деятельности, общения и социальных отношений, максимально быстро адаптироваться в конкретной культурной среде.

В качестве основных составляющих функциональной грамотности выделяют: математическую грамотность, читательскую грамотность, естественно-научную грамотность, финансовую грамотность, глобальные компетенции и креативное мышление. Реализация данной задачи осуществляется за счет использования заданий, разработанных на основе системно-деятельностного подхода. Такие задания будут способствовать формированию и оценке способности личности применять полученные знания для решения различных учебных и практических задач.

Формирование функциональной грамотности реализуется на основе личностных, метапредметных и предметных результатов освоения учебного предмета.

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;

сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные.

Регулятивные универсальные учебные действия.

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 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;

Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:
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.

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:
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, со-здание 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.

Предметные:

Выпускник научится:

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.

Выпускник овладеет:

приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Выпускник получит возможность овладеть:

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 источники информации, включая Интернет-ресурсы и другие базы данных.

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.

Содержание курса внеурочной деятельности

Модуль 1. «Информационная безопасность»

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 7-9 классов. Рекомендуется для реализации в рамках внеурочной деятельности обучающихся.

В преподавании модуля «Информационная безопасность» могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат.

Система учебных заданий должна создавать 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 (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы и т.д.).

Программа учебного курса (Модуль 1) рассчитана на 34 учебных часа, из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение. На изучение модуля 1 «Информационная безопасность» отводится по 1 часу в неделю в 7, 8 или 9 классах. Учебные занятия по программе могут быть реализованы в различных вариантах:

1. в течение одного учебного года в 7, 8 или 9 классах. В этом случае программа рассчитана на 34 учебных часа;
2. по одному разделу последовательно в 7, 8 и 9 классах;
3. произвольно распределены учителем в зависимости от интереса и готовности школьников.

Содержание программы учебного курса (Модуль 1).

Содержание программы учебного курса (Модуль 1) соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

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

Каждый раздел учебного курса (Модуля 1) завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

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.

Содержание учебного курса (Модуль 1).

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 кибер-буллинга.

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 об-наружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ. 2 часа.

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.

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.

Повторение. Волонтерская практика. 3 часа.

Тематическое планирование

Согласно учебному плану ГБОУ ООШ № 19 на реализацию программы внеурочной деятельности «Информационная безопасность» в 7-9 классах отводится 1 час в неделю, итого 34 часа в год.

Тематическое планирование учебного курса (Модуль 1).

№п/п	Содержание	Планируемое количество часов	
		теоретических	практических
1	Тема 1. «Безопасность общения»	13	
		6	7
2	Тема 2. «Безопасность устройств»	8	
		5	3
3	Тема 3 «Безопасность информации»	13	
		7	6
Итого		34	

Модуль 2.

При работе с родителями важнейшей задачей является преодоление «цифрового разрыва» и обучение родителей правильной оценке своих возможностей в помощи детям в Интернете – возможностей, которые достаточно велики.

Разработчики курса предполагают, что родители с большей готовностью включатся в программу развития цифровой гигиены, предлагающую им общение, совместный поиск и развивающие игры и т.п.

Вместе с тем, формами проведения мероприятий для родителей также могут являться: лектории, выступления на родительских собраниях, микро-обучение на основе технологий онлайн обучения, геймификация, создание чек-листов, совместное обучение, совместные родительско-детские проекты и пр.

Практические материалы для реализации данного модуля представлены в приложении 2 к данной рабочей программе. Разработчики курса «Цифровая гигиена» предлагают использовать вышеуказанное приложение в качестве конструктора при подготовке к мероприятиям.

Тематическое планирование учебного курса (Модуль 2).

Тема 1. История возникновения Интернета. Понятия Интернет-угроз. Изменения границ допустимого в контексте цифрового образа жизни

Тема 2. Изменения нормативных моделей развития и здоровья детей и подростков.

Тема 3. Цифровая гигиена: зачем это нужно? Понятие периметра безопасности. Обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребенка. Баланс ценностей развития и ценностей безопасности.

Тема 4. Угрозы информационной безопасности: атаки, связанные с компьютерной инженерией. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 5. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Груминг, кибербуллинг. Чему мы должны научить ребёнка для профилактики насилия в Сети?

Тема 6. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Фишинг. Обращение с деньгами в сети Интернет. Детская пластиковая карта: быть или не быть?

Тема 7. Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ.

Тема 8. Пособия и обучающие программы по формированию навыков цифровой гигиены.

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 осмысливается 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 ИТ-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, про-граммный продукт, стенд, статья, наглядное пособие, литературное произве-дение, видео-ролик, мультфильм и т.д.).
6. Умение установить отношения коллаборации с участниками проекта, наме-тить пути создания сетевого продукта. Способность намечать пути сотрудни-чества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации коммуникабельности, благодарности и уважения по отно-шению к руководи-телю, консультантам, умение четко обозначить пути созда-ния сетевого продукта.
7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.

Список источников:

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2019. – 182 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2019. – 384 с.
4. Дети в информационном обществе // <http://detionline.com/journal/about>
5. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ-ДАНА, 2019. – 239 с.
6. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с.
7. Защита детей by Kaspersky // <https://kids.kaspersky.ru/>
8. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Ру-сайнс, 2020. – 64 с.
9. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.
10. Основы кибербезопасности. // <https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa>
11. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон. научн. журн. 2019. № 22(66)