



**государственное автономное профессиональное
образовательное учреждение Самарской области
«Самарский колледж сервиса производственного оборудования
имени Героя Российской Федерации
Е.В. Золотухина»**

УТВЕРЖДАЮ
Приказ директора колледжа
от 25.05.2021 г. № 119/1

**РАБОЧАЯ ПРОГРАММА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**
программа основного общего образования

2021 г.

Пояснительная записка

Программа курса внеурочной деятельности «Информационная безопасность» для 8 классов разработана в соответствии с требованиями Федерального государственного образовательного стандарта основного общего образования (ФГОС ООО), Основной образовательной программы основного общего образования ГАПОУ СКСПО, примерной образовательной программы учебного курса «Информационная безопасность» для образовательных организаций, реализующих программы основного общего образования (Москва, протокол от 26.10.2020 №4/20), авторской программы Наместниковой М.С.

«Информационная безопасность, или На расстоянии одного вируса» (М., Просвещение, 2019).

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. Кроме того, реализация курса создает условия для сокращения цифрового разрыва между поколениями и позволяет родителям выступать в качестве экспертов, передающих опыт.

Отбор тематики содержания курса осуществлен с учетом возрастных особенностей и познавательных возможностей обучающихся 8-х классов.

Программа курса внеурочной деятельности рассчитана на 34 часа в год (по 1 часу в неделю).

Цель и задачи изучения

Основными целями изучения курса внеурочной деятельности «Информационная безопасность» являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре обучающихся, 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.

Планируемые результаты освоения курса внеурочной деятельности

Личностные результаты:

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

Метапредметные результаты:

Регулятивные универсальные учебные действия.

Выпускник научится:

- 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.

Выпускник получит возможность:

- 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.

Познавательные универсальные учебные действия

Выпускник 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.

Выпускник получит возможность:

- 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

Выпускник 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.

Выпускник получит возможность:

- использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуника-

ционных 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.

Предметные результаты:

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

Выпускник получит возможность научиться:

- основам соблюдения норм информационной этики и права;
- основам 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.

Данная программа предполагает 1-2 уровни воспитательных результатов.

Воспитательные результаты:

Первый уровень (приобретение школьником социальных знаний) - приобретение обучающимися знаний о правилах пользования компьютером; о способах нахождения и обработки информации и защите своих персональных данных в социальных сетях.

Второй уровень (получение школьником опыта переживания и позитивного отношения к базовым ценностям общества) - школьник может приобрести опыт публичного выступления, проведения опросов обучающихся школы, родителей, учителей; опыт общения, чувства ответственности за других людей, опыт управления другими людьми, развитие ценностных отношений к своему здоровью и внутреннему миру.

Тематическое планирование

№ № п/п	Название раздела	Часы аудиторных занятий	Часы практических занятий (не менее 50%)	Общее кол-во часов
1.	Безопасность общения	7	6	13
2.	Безопасность	3	4	7

	устройств			
3.	Безопасность информации	7	7	14
	ИТОГО	17 (50%)	17 (50%)	34 (100%)

Содержание программы

№	Название темы	Краткое содержание темы	Формы организации образовательного процесса
Безопасность общения			
1	Общение в социальных сетях и мессенджерах	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	Беседа
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.	Объяснение
3	Пароли для аккаунтов социальных сетей	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Видеоролик
4	Безопасный вход в аккаунты	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	Беседа
5	Настройки конфиденциальности в социальных сетях	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Практическая работа
6	Публикация информации в социальных сетях	Персональные данные. Публикация личной информации.	Объяснение
7	Кибербуллинг	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Видеоролик
8	Публичные аккаунты	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Беседа
9	Публичные аккаунты	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Видеоролик
10	Фишинг	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	Видеоролик
11-13	Работа над индивидуальными проектами	Выполнение и защита индивидуальных и групповых проектов	Групповая

№	Название темы	Краткое содержание темы	Формы организации образовательного процесса
Безопасность устройств			
14	Что такое вредоносный код	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Беседа
15	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.	Обсуждение
16 - 17	Методы защиты от вредоносных программ	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	Объяснение
18	Распространение вредоносного кода для мобильных устройств	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Видеоролик
19 - 21	Работа над индивидуальными проектами	Выполнение и защита индивидуальных и групповых проектов	Групповая
Безопасность информации			
22	Социальная инженерия: распознать и избежать	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Беседа
23	Ложная информация в Интернете	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Видеоролик
24	Безопасность при использовании платежных карт в Интернете	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Видеоролик
25	Беспроводная технология связи	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Практикум
26	Резервное копирование данных	Безопасность личной информации. Создание резервных копий на различных устройствах.	Практикум
27 - 28	Основы государственной политики в области формирования культуры информационной безопасности	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.	Беседа
29 - 30	Работа над индивидуальными проектами	Выполнение и защита индивидуальных и групповых проектов	Групповая
31	Повторение. Волонтерская практика	Проведение занятий для обучающихся 4-6 классов.	Групповая

№	Название темы	Краткое содержание темы	Формы организации образовательного процесса
34			

Формы диагностики и подведения итогов

В итоге изучения материала обучающиеся пишут рефераты, выступающие в качестве итоговой практической работы. Контроль за изученным материалом осуществляется в форме тематических рисунков, кроссвордов, презентаций, тестов, рефератов, устных ответов, собеседования. Текущий контроль за усвоением материала осуществляется на каждом занятии посредством мини-опроса и выполнения практических заданий.