Комитет образования администрации
Полтавского муниципального района Омской области
Бюджетное общеобразовательное учреждение Полтавского муниципального района Омской области «Ольгинская средняя школа»

Принята на заседании методического (педагогического) совета СШ»
от «_29_» _марта_2024 г.
Протокол № _6_

Утверждаю:
Директор БОУ «Ольгинская
_____/Давальченко Е.В./
«_29_» ___03___ 2024 г.

Дополнительная общеобразовательная общеразвивающая программа технической направленности

«Информационная безопасность»

Возраст обучающихся: 13-17 лет
Срок реализации: 3 года
Трудоемкость программы: 108 часов
Форма обучения: очная с применением ДОТ
Уровень сложности: *базовый уровень*

Автор составитель: Толкова Вера Дмитриевна, педагог дополнительного образования

Ольгино, 2024

Пояснительная записка

Дополнительная общеобразовательная общеразвивающая программа «Информационная безопасность» (далее – Программа) технической направленности, реализуемая в очной форме с применением дистанционных образовательных технологий посредством ГИС «Навигатор».

Программа предназначена для обучения подростков, 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.

Программа носит практико-ориентированный характер и направлена на приобретение умений ориентироваться в мире информационных технологий, способствует принятию грамотных решений, минимизирует риски и тем самым способно повысить их информационную безопасность. Реализация данной Программы создаёт благоприятные условия для формирования культуры поведения, самостоятельности, ответственности запринятие решения.

Актуальность Программы

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.

Особенности организации образовательного процесса

Все содержание программы реализуется в режиме онлайн (реального времени) по утвержденному педагогом расписанию занятий посредством платформы ГИС «Навигатор дополнительного образования детей Омской области» в модулях «Вебинары», «Занятия» и «Проверочные задания».

Данная форма обучения позволяет:

- увеличить охват обучающихся;
- обучать детей, находящихся в отдаленности от организации дополнительного образования;
- проводить обучение в условиях ограничения посещения организации дополнительного образования (карантин, самоизоляция).

Психолого-педагогические характеристики, особенности 13-17 летних детей.

Подростковый возраст - сложный ответственный период становления личности (по Л. Божович, это период второго рождения личности), в котором формируется социальная направленность и моральное сознание: моральные взгляды, суждения, оценки, представления о нормах поведения, заимствованные у взрослых овладение ими происходит через реальные отношения, через оценку их деятельности взрослыми. Например, сразу подростки осознают, что волю закаляет и обучение, открытое признание своих ошибок свидетельствует о смелости, что осознание своей вины - шаг к ответственности. Знание моральных норм и эталонов взаимоотношений понимают не всегда глубоко, трудно воспринимают моральный релятивизм, поэтому оценки поступков других категоричны, бескомпромиссные. Моральные убеждения еще не являются неустойчивыми, однако они становятся специфическими мотивами поведения. Появляются собственные взгляды, оценки, которые могут быстро измениться, но и противоположный взгляд подросток будет отстаивать так же страстно.

Важные изменения происходят в мотивационной сфере: потребность в самоуважении, в самоутверждении, в признании товарищей, в положительном отношении со стороны друзей. Появляется ориентация на будущее: мечты, идеалы, перспективные планы, отдаленная цель. Однако для подростка характерно и отказ от поставленной цели вопреки ее объективной значимости, ибо воля еще слаба. Подростки чаще действуют по наиболее сильным мотивам, собственным же поведением они еще не способны управлять в полной мере, и признают отсутствие у себя волевых качеств. В подростковом возрасте возрастает познавательная активность и расширяются границы заинтересованности. Обучающиеся начинают задумываться над вопросами, которые до сих пор их не волновали: о жизни и смерти, о чувствах и о взаимоотношениях между людьми.

Подростки находятся на той стадии социализации, когда действуют механизмы не только усвоение социального опыта через наблюдение, подражание, адаптацию, но и активного преобразования материальной и духовной культуры. Поэтому столь привлекательным для них мир социальных сетей, где создана иллюзия реального мира, погрузившись в который, обучающийся может реализовать свои потребности.

Педагогическая целесообразность

Обучение по Программе позволит обучающимся ознакомиться с основами информационной безопасности, получить практические навыки. Это необходимо предоставить молодёжи уже на этапе школьного образования. Так же педагогическая целесообразность заключается в применяемом на занятиях деятельностном подходе, который позволяет максимально продуктивно усваивать материал путём смены способов организации работы. Тем самым педагог стимулирует познавательные интересы обучающихся и развивает их практические навыки. У обучающихся воспитываются ответственность за свою работу, аккуратность, взаимовыручка. В программу включены коллективные практические занятия, развивающие коммуникативные навыки и способность работать в команде. Практические занятия помогают развивать у обучающихся внимание, концентрацию на своих действиях в сети Интернет, умение обеспечивать информационную безопасность свою и своих близких. Часть учебного времени отведена на проектную деятельность - совместную учебно-познавательную, творческую деятельность, имеющую общую цель, согласованные методы, способы деятельности, направленные на достижение общ его результата. Тематика каждого из созданных обучающимися проектов будет направлена на сохранение информационной безопасности в направлениях изучаемых модулей. Непременным условием проектной деятельности является наличие заранее выработанных представлений о ее конечном продукте и, как следствие этого, этапах проектирования и реализации проекта, включая его осмысление и рефлексию результатов деятельности. Так как «образование - единый целенаправленный процесс воспитания и обучения, являющийся общественно значимым благом и осуществляемый в интересах человека, семьи, общества и государства...»

Поэтапное освоение Программы способствует пониманию информационно-телекоммуникационных терминов, а также многогранности виртуального и информационного мира, даёт возможность задуматься над своей виртуальной безопасностью.

Характеристика целевой группы: Подростковый возраст всегда вызывал и у родителей, и у педагогов особую тревогу, как возраст проявления рискованного поведения. И сегодня эта тема не потеряла своей актуальности. Подростки — активные пользователи интернета. Зачастую, обучающиеся подросткового возраста в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети. Сделать их пребывание в интернете более безопасным, научить их ориентироваться в киберпространстве — важная задача для педагогов.

Трудоёмкость программы - 108 часов: 1 год обучения - 36 часов, 2 год обучения - 36 часов, 3 год обучения – 36 часов.

Занятия проводятся 1 раз в неделю по 1 часу.

Форма и режим занятий: очное обучение с применением дистанционных образовательных технологий.

Количество обучающихся в группе до 15 человек.

В группы принимаются все желающие, подавшие заявки через ГИС «Навигатор»

Цель программы: формирование информационной культуры обучающихся посредством изучения базовых принципов безопасного поведения в сети «Интернет».

Реализация поставленной цели осуществляется при решении следующих **задач:**

- сформировать навыки ответственного и безопасного поведения в современной информационно-телекоммуникационной среде;
- 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.

Планируемые результаты освоения программы:

Личностные

- осознанно и уважительно относятся к окружающим людям в реальном и виртуальном мире, их позициям, взглядам;
- готовы и умеют вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
- знает правила индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные

- ставят цель деятельности на основе определенной проблемы и существующих возможностей;
- выдвигают версии решения проблемы, предвосхищая конечный результат;
- излагают полученную информацию, интерпретируя ее в контексте решаемой задачи;
- осуществляют взаимодействие с электронными поисковыми системами, словарями;
- формируют множественную выборку из поисковых источников для объективизации результатов поиска;
- строят позитивные отношения в процессе учебной и познавательной деятельности;
- представляют в устной или письменной форме развернутый план собственной деятельности;

Предметные

- безопасно используют ресурсы Интернета;
- анализируют доменные имена компьютеров и адреса документов в интернете;
- применяют способы самозащиты при попытке мошенничества;
- владеют приемами безопасной организации своего личного информационного пространства с использованием индивидуальных накопителей данных, интернет-сервисо

Учебно-тематический план 1 года обучения

№ п/п	*Разделы и темы учебных занятий*	*Количество часов*
Раздел 1. Общение в социальных сетях и мессенджерах		**6**
Тема 1.1.	Введение в программу	**1**
Тема 1.2.	Социальная сеть.	1
Тема 1.3.	История социальных сетей	1
Тема 1.4.	Мессенджеры.	1
Тема 1.5.	Назначение социальных сетей и мессенджеров.	1
Тема 1.6.	Пользовательский контент.	1
Раздел 2. С кем безопасно общаться в интернете		**3**
Тема 2.1.	**Правила добавления друзей в социальных сетях**	1
Тема 2.2.	Профиль пользователя.	1
Тема 2.3.	Анонимные социальные сети.	1
Раздел 3. Методы защиты от вредоносных программ		**4**
Тема 3.1.	Сложные пароли.	1
Тема 3.2.	Онлайн генераторы паролей	1
Тема 3.3.	Правила хранения паролей	2
Тема 3.4.	Использование функции браузера по запоминанию паролей	1
Раздел 4. Безопасный вход в аккаунты		**3**
Тема 4.1.	Виды аутентификации.	1
Тема 4.2.	Настройки безопасности аккаунта	1
Тема 4.3.	Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	1
Раздел 5. Настройки конфиденциальности в социальных сетях		**2**
Тема 5.1.	Настройки приватности и конфиденциальности в разных социальных сетях.	1
Тема 5.2.	Приватность и конфиденциальность в мессенджерах.	1
Раздел 6. Публикация информации в социальных сетях		**2**
Тема 6.1.	**Персональные данные.**	1
Тема 6.2.	**Публикация личной информации.**	1
Раздел 7. Кибербуллинг		**4**
Тема 7.1.	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать?	2
Тема 7.2.	Как не стать жертвой кибербуллинга.	1
Тема 7.3.	Как помочь жертве кибербуллинга.	1
Раздел 8. Публичные аккаунты		2
Тема 8.1.	Настройки приватности публичных страниц.	1
Тема 8.2.	Правила ведения публичных страниц	1
Раздел 9. Фишинг		4
Тема 9.1.	Фишинг как мошеннический прием.	
Тема 9.2.	Популярные варианты распространения фишинга.	
Тема 9.3.	Отличие настоящих и фишинговых сайтов.	
Тема 9.4.	Как защититься от фишеров в социальных сетях и мессенджерах.	
Раздел 10. Выполнение и защита индивидуальных и групповых проектов		6
Тема 10.1.	**Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта.**	1

Тема 10.2.	**Цели, задачи, работа над проектом. Защита проекта.**	4
Тема 10.3.	**Итоговое занятие**	**1**
Итого:		**36**

Учебно-тематический план 2 года обучения

№ п/п	***Разделы и темы учебных занятий***	***Количество часов***
Раздел 1. Что такое вредоносный код		**8**
Тема 1.1.	Введение в программу	1
Тема 1.2.	Виды вредоносных кодов.	3
Тема 1.3.	Возможности и деструктивные функции вредоносных кодов.	4
Раздел 2. Распространение вредоносного кода		**12**
Тема 2.1.	Способы доставки вредоносных кодов.	2
Тема 2.2.	Исполняемые файлы и расширения вредоносных кодов.	2
Тема 2.3.	Вредоносная рассылка.	2
Тема 2.4.	Вредоносные скрипты.	2
Тема 2.5.	Способы выявления наличия вредоносных кодов на устройствах.	2
Тема 2.6.	Действия при обнаружении вредоносных кодов на устройствах.	2
Раздел 3. Методы защиты от вредоносных программ		**6**
Тема 3.1.	Способы защиты устройств от вредоносного кода.	2
Тема 3.2.	Антивирусные программы и их характеристики.	2
Тема 3.3.	Правила защиты от вредоносных кодов.	2
Раздел 4. Распространение вредоносного кода для мобильных устройств		**4**
Тема 4.1.	Расширение вредоносных кодов для мобильных устройств.	2
Тема 4.2.	Правила безопасности при установке приложений на мобильные устройства.	2
Раздел 5. Выполнение и защита индивидуальных и групповых проектов		**6**
Тема 5.1.	**Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта.**	1
Тема 5.2.	**Цели, задачи, работа над проектом. Защита проекта.**	4
Тема 5.3.	**Итоговое занятие**	1
Итого:		**36**

Учебно-тематический план 3 года обучения

№ п/п	***Разделы и темы учебных занятий***	***Количество часов***
Раздел 1. Социальная инженерия: распознать и избежать		**8**
Тема 1.1.	Введение в программу	1
Тема 1.2.	Приемы социальной инженерии.	4
Тема 1.3.	Правила безопасности в виртуальных контактах.	4
Раздел 2. Ложная информация в Интернете		**5**

Тема 2.1.	Фейковые новости	3
Тема 2.2.	Поддельные страницы	2
Раздел 3. Безопасность при использовании платежных карт в Интернете		**6**
Тема 3.1.	Транзакции и связанные с ними риски.	2
Тема 3.2.	Правила совершения онлайн покупок	2
Тема 3.3.	Безопасность банковских сервисов	2
Раздел 4. Беспроводная технология связи		**5**
Тема 4.1.	Уязвимости Wi-Fi-соединений.	1
Тема 4.2.	Публичные и непубличные сети.	2
Тема 4.3.	Правила работы в публичных сетях.	2
Раздел 5. Резервное копирование данных		**5**
Тема 5.1.	Безопасность личной информации.	2
Тема 5.2.	Создание резервных копий на различных устройствах.	3
Раздел 6. Выполнение и защита индивидуальных и групповых проектов		**6**
Тема 6.1.	**Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта.**	1
Тема 6.2.	**Цели, задачи, работа над проектом. Защита проекта.**	4
Тема 6.3.	**Итоговое занятие**	1
Итого:		**36**

Содержание программы 1 года обучения

Раздел 1. Общение в социальных сетях и мессенджерах - 6 ч.

Тема 1.1. Введение в программу. - 1 ч.

Знакомство с понятием и видами денег (наличные, электронные и т.д.), историей их возникновения и развития в формате видео лекции через модуль «Занятия» по ссылке на видео материал. Разбор четырех основных функций денег в процессе беседы, организованной через модуль «Вебинары».

Знакомство с правилами внутреннего распорядка образовательной организации, правилами ТБ. Организация рабочего места, беседа организованна через модуль «Вебинары». Разберемся в понятиях: «информационная безопасность», «информационная грамотность», «информационный иммунитет», «медиаграмотность», организуется через модуль «Занятия» по ссылке на теоретический материал. Просмотр презентации «Что такое «Информационная безопасность?», организованной через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – составление кроссворда «Информационная безопасность»

Тема 1.2. Социальная сеть. – 1 ч.

Знакомство с понятием социальные сети, организуется через модуль «Занятия» по ссылке на теоретический материал. Рассмотреть «плюсы» и «минусы» социальных сетей. Рассмотреть, как социальные сети влияют на мозг человека и его реальную жизнь – дискуссия организуется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – выполнение практической работы по составлению сравнительной таблицы.

Тема 1.3. История социальных сетей. – 1 ч.

Познакомиться с историей социальных сетей. Просмотр видеоролика в формате видео лекции через модуль «Занятия» по ссылке на видео материал. Развитие социальных сетей, беседа и обсуждение, организованы через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – тест.

Тема 1.4. Мессенджеры. – 1 ч.

Познакомится с историей цифровых сервисов для общения, с основными принципами цифрового этикета, а также изучите технологии, которые применяются в мессенджерах: от чат-ботов до нейросетей, которые расшифровывают аудиосообщения, организуется через модуль «Занятия» по ссылке на теоретический материал.

Прохождение тренажёра «Мессенджеры» на платформе «Урок Цифры»

Форма контроля: осуществляется через модуль «Проверочные задания» – сертификат о прохождении тренажёра.

Тема 1.5. Назначение социальных сетей и мессенджеров. – 1 ч.

Рассмотреть популярные мессенджеры - организуется через модуль «Занятия» по ссылкам на социальные сети. Определить влияние социальных сетей на безопасность человека в ходе дискуссии, организованной через модуль «Вебинары». Обсуждение вопросов о значимости социальных сетей в жизни человека.

Форма контроля: осуществляется через модуль «Проверочные задания» – тест по результатам дискуссии.

Тема 1.6. Пользовательский контент. – 1 ч.

Познакомиться с понятием «контент», классификацией по содержанию и целям, организуется через модуль «Занятия» по ссылке на теоретический материал. Основные типы и форматы размещения информации в социальных сетях. Какой вид контента выбрать исходя из целей? Участие в беседе, организуется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – предоставление творческого отчета «Мой контент» (статья, видео ролик, сторис, и т.д.).

Раздел 2. С кем безопасно общаться в Интернете. - 3 ч.

Тема 2.1. Правила добавления друзей в социальных сетях. - 1 ч.

Возможности социальных сетей для установления связей с другими людьми, демонстрация рисков, связанных с общением с незнакомцами в Интернете; выделение признаков, на которые следует обращать внимание при знакомстве с другими людьми в Интернете; изучение правил поведения, которых следует придерживаться при общении с незнакомцами в Интернете, организуется через модуль «Занятия» по ссылке на теоретический материал ; поиск способов, как обезопасить себя при встрече в реальной жизни с интернет-знакомыми – дискуссия организуется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – создание памятки.

Тема 2.2. Профиль пользователя. - 1 ч.

Знакомство с понятием «Пользовательский профиль», изучение статьи «Создаем пользовательский профиль», через модуль «Занятия» по ссылке на теоретический материал.

Практическая работа «Управление профилями пользователей» контент- платформа https://pandia.ru/text/78/213/92463.php

Форма контроля: осуществляется через модуль «Проверочные задания» – практическая работа.

Тема 2.3. Анонимные социальные сети. – 1 ч.

Узнаем, что такое анонимные сайты. Степени анонимности. Противоречие. Перспективы использования. Доход от анонимных социальных сетей. Анонимные приложения. Анонимные сайты. Ознакомление с теоретическим материалом через модуль «Занятия» по ссылке, участие в обсуждении через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – выполнение практической работы по составлению сравнительной таблицы.

Раздел 3. Пароли для аккаунтов социальных сетей. - 4 часа.

Тема 3.1. Сложные пароли. – 1 ч.
Знакомство понятием «пароль». Правильная комбинация пароля и информационная безопасность. Способы получения паролей. Примеры программ для взлома паролей. Ознакомление с материалом происходит через
Форма контроля: осуществляется через модуль «Проверочные задания» –практическое задание по выполнению эстафеты знаний.

Тема 3.2. Онлайн генераторы паролей. – 1 ч.
Знакомство с Языком программирования Python. Узнаем, что такое инструменты для разработки программы, ознакомление осуществляется через модуль «Задания» в виде ссылки не теоретический материал. Разработка и тестирование программы генератора паролей - освоение через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – выполнение практической работы по создание надежного пароля с помощью приложения.

Тема 3.3. Правила хранения паролей. – 1 ч.
Узнаем правила безопасной аутентификации, защите личной информации в сети Интернет, освоение материала осуществляется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – выполнение творческой работы по создание буклета

Тема 3.4. Использование функции браузера по запоминанию паролей. – 1 ч.
Ознакомление и выявление основных причин не хранить пароли в браузерах, а использовать для этого более безопасный метод хранения — отдельный менеджер паролей. Вредоносное ПО — стилеры паролей. Главная проблема хранения паролей в браузерах, дискуссия организована через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – практическая работа «Пароли в моем телефоне»

Раздел 4. Безопасный вход в аккаунты. - 3 часа.

Тема 4.1. Виды аутентификации. - 1 ч.
Знакомство с теоретическим материалом: Виды аутентификации. Аутентификации: с помощью пароля, специального слова или кода, с помощью специального устройства, физического носителя, с помощью биометрических данных, сквозная. Правила безопасной аутентификации, ознакомление с информацией по ссылке в модуле «Задания». Защита личной информации в сети Интернет – организовано через участие в беседе модуля «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – выполнение теста по теме.

Тема 4.2. Настройки безопасности аккаунта. – 1 ч.
Знакомство обучающихся со следующей информацией: что Вы знаете о взломах аккаунта, как уберечь аккаунт в социальной сети от взлома, как сохранить свой аккаунт, осуществляется через просмотр видеоматериалов, размещённых в модуле «Задания» ГИС «Навигатор дополнительного образования» по ссылке на видеоматериал.

Форма контроля: настройка безопасности аккаунта в своих социальных сетях – предоставление ссылки для проверки безопасности.

Тема 4.3. Работа на чужом компьютере с точки зрения безопасности личного аккаунта. - 1 ч.
Ознакомление со списком типичных паролей любого пользователя. Выявление связи навыков повседневного использования интернета и электронных устройств с правилами безопасности. Формирование у обучающихся навыков безопасного использования Интернета на основании имеющегося у них опыта.
Повышение уровня осведомленности детей о наиболее актуальных Интернет-угрозах. Участие в беседе, организованной через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – выполнение

творческой работы по создание буклета

Раздел 5. Настройки конфиденциальности в социальных сетях. - 2 часа.

Тема 5.1. Настройки приватности и конфиденциальности в разных социальных сетях. - 1 ч.
Изучение собственного баланса «открытости — закрытости», знакомство с основными настройками приватности в сети. Выполнение упражнения «Золотая середина». Выполнение упражнения «Моя приватность в сети» освоение материала осуществляется через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – выполнение творческой работы «НАСТРОЙКИ ПРИВАТНОСТИ»

Тема 5.2. Приватность и конфиденциальность в мессенджерах. – 1 ч.
Ознакомление с теоретическими знаниями «Основные риски пересылки личных данных через мессенджеры», «Основные функции и настройки конфиденциальности в мессенджерах», организовано через модуль «Занятия». Знакомство с определением «социальная инженерия» и взаимосвязь понятия «Утечка конфиденциальности информации в мессенджерах» - дискуссия, организованная в модуле «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – разработка списка практических советов для сохранения личной информации и обеспечения конфиденциальности в мессенджерах во время использования общедоступных Wi-fi сетей.

Раздел 6. Публикация информации в социальных сетях. - 2 часа.

Тема 6.1. Персональные данные. - 1 ч

Знакомство обучающихся с теоретическими материалами по теме «Персональные данные» посредством модуля «Задания». Проанализировать и сформировать общие принципы безопасного поведения в сети Интернет и защиты персональных данных, через участие в беседе, организованной в модуле «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – тестирование

Тема 6.2. Публикация личной информации. – 1 ч.
Актуализация знаний о понятии «Публикация информации в сети Интернет». Повторение основных сервисов публикации информации в сети Интернет. Научить обучающихся правильно публиковать различные виды информации в сети Интернет, освоение данной темы осуществляется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – практическое задание «Публикация статьи»

Раздел 7. Кибербуллинг. - 4 часа.

Тема 7.1. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? – 2 ч.
Знакомство с понятием кибербуллинга; актуализация знаний о правилах безопасной работы в сети Интернет; сформировать умение анализировать и систематизировать теоретическую информацию, представленную в модуле «Занятия»; Дискуссия по теме организуется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – выполнение теста «Интернет-омут».

Тема 7.2. Как не стать жертвой кибербуллинга. – 1 ч.
Ознакомление с теоретическими знаниями «Принципы создания условий для безопасности обучающихся, предупреждение негативных явлений в семье, школе, ближайшем окружении в реальном и виртуальном пространстве». Дискуссия, организованная через

модуль «Вебинары» нацелена на формирование навыка безопасного поведения в сети Интернет. Знакомство с правилами общения в Интернете.
Форма контроля: осуществляется через модуль «Проверочные задания» – выполнение творческой работы по созданию буклета.

Тема 7.3. Как помочь жертве кибербуллинга. – 1 ч.

Ознакомление обучающихся с теоретическими основами понятий: «Общие правила безопасного поведения ребенка в сети Интернет», «Методы борьбы с кибербуллингом», «Закон против кибербуллинга», через ГИС Навигатор модуль «Занятия». Участие в беседе по темам: «Как помочь ребенку, ставшему жертвой кибербуллинга», «Как поддержать ребенка, ставшего жертвой кибербуллинга», «Профилактика кибербуллинга», через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – выполнение творческой работы по создание буклета «Я в социальных сетях»

Раздел 8. Публичные аккаунты. – 2 ч.

Тема 8.1. Настройки приватности публичных страниц. – 1 ч.

Познакомить обучающихся с основами информационной безопасности и важным навыком 21 века — умением защищать свои персональные данные, через просмотр Видеоурока «Приватность в социальных сетях, ссылка на видеоматериал размещена в модуле «Занятия», практическая работа - тренажёр «Приватность в цифровом мире» https://урокцифры.рф/lessons/cybersecurity
Форма контроля: размещение сертификата о прохождении тренажёра.

Тема 8.2. Правила ведения публичных страниц. – 1 ч.

Ознакомление и формирование знаний о приватности и персональных данных, а также способах попадания данных в Интернет и их распространения в сети. Управление персональными данными при работе с различными онлайн-ресурсами, приложениями и устройствами путём просмотра обучающего видеоурока «Публичные и приватные страницы», ссылка на который размещается в модуле «Занятия».
Форма контроля: осуществляется через модуль «Проверочные задания» – ответы на вопросы викторины

Раздел 9. Фишинг. – 4 часа.

Тема 9.1. Фишинг как мошеннический прием. – 1 ч.

Знакомство с понятием «Фишинг», видами фишинговых финансовых мошенничеств, теоретические аспекты представлены в модуле «Занятия». Практическое закрепление навыков выработки личной стратегии грамотного поведения в ситуациях растущих финансовых рисков и мошенничестве в ходе дискуссии, организованной через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – опрос

Тема 9.2. Популярные варианты распространения фишинга. – 1 ч.

В ходе изучения теоретических материалов, размещённых в модуле «Занятия», обучающиеся познакомятся с понятиями: «Почтовый фишинг», «Спеарфишинг или целевой фишинг», «Уэйлинг», «Смишинг», «Вишинг», «BCO», «CEO-мошенничество», «Компрометация корпоративной электронной почты», «Клон-фишинг», «Фишинг-атака «злой двойник», «Фишинг в социальных сетях», «Фишинг в поисковых системах», «Фарминг». После ознакомления с теорией обсудят данные понятия в форме видеоконференции через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – подготовить Памятку «Советы по обнаружению и предотвращению фишинговых атак»

Тема 9.3. Отличие настоящих и фишинговых сайтов. – 1 ч.

В ходе дискуссии, организованной через модуль «Вебинары» обучающиеся смогут ответить на следующие вопросы: как мошенники заманивают пользователей на

фишинговые сайты? Какие сайты подделывают мошенники? Как распознать фишинговый сайт?
Форма контроля: осуществляется через модуль «Проверочные задания» – опрос
Тема 9.4. Как защититься от фишеров в социальных сетях и мессенджерах. – 1 ч.
Познакомятся с понятием кражи личных данных, интернет-мошенничеством, фишингом, понятием личной информации, укороченными URL, освоение материалов через просмотр видео урока «Социальные сети, мессенджеры и почтовые сервисы. Фейки и фишинг», ссылка на видеоматериал размещается в модуле «Занятия».
Форма контроля: осуществляется через модуль «Проверочные задания» – разработка рекомендации «Как защититься от фишинга в социальных сетях и мессенджерах»

Раздел 10. Выполнение и защита индивидуальных и групповых проектов. – 6 часов.
Тема 10.1. Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. – 1 ч.
Знакомство с теоретическими аспектами проектной деятельности, типами и видами проектов, основными этапами разработки проектов и их назначением, организуется через модуль «Занятия».
Форма контроля: осуществляется через модуль «Проверочные задания» – составление паспорта проекта
Тема 10.2. Цели, задачи, работа над проектом. Защита проекта. – 4 ч.
Изучение теоретического материала по теме, организуется через ссылку на теоретический материал.
Выделение проблемы, постановка целей и задач исследования. Формулировка гипотезы. Освоение методики исследования. Сбор собственного материала. Обработка собранного материала. Обобщение, анализ, выводы. Представление исследовательской работы, консультация по подготовке проекта осуществляется через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – представление проектной папки.
Тема 10.3. Итоговое занятие. – 1 ч.
Подведение итогов года, видео встреча организуется через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – выставка фотографий проектных работ.

Содержание программы 2 года обучения

Раздел 1. Что такое вредоносный код. - 8 часов.
Тема1.1. Введение в программу. - 1 ч.
Знакомство с правилами внутреннего распорядка, правилами ТБ. Организация рабочего места. в понятиях: «информационная безопасность», «информационная грамотность», «информационный иммунитет», «медиаграмотность». Просмотр и анализ презентации «Информационная безопасность», организованных через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – составление кроссворда «Информационная безопасность».
Тема 1.2. Виды вредоносных кодов. – 3 ч.
Ознакомление с историей и классификацией вирусов, общими принципами действия компьютерных вирусов, организуется через модуль «Занятия» путём отработки теоретических материалов и просмотра видеоурока «Виды вредоносного программного обеспечения». Обсуждение темы «Вредоносные программы», организованных через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – опрос
Тема 1.3. Возможности и деструктивные функции вредоносных кодов. – 4 ч.

Знакомство с технологиями, применяемые в деструктивных вредоносных программах, удаление файлов по заданным условиям, рекурсивное удаление или повреждение всех файлов на диске, низкоуровневое повреждение данных на жестком диске, нарушение функционирования операционной системы при помощи правки реестра, Причины создания деструктивных троянских программ и их задачи, ознакомление с теорией осуществляется посредством модуля «Занятия». Обсуждение и практическая отработка знаний, организованны через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – подготовка кроссворда «Вредоносные программы»

Раздел 2. Распространение вредоносного кода. – 12 часов.

Тема 2.1. Способы доставки вредоносных кодов. – 2 ч.

Ознакомление с теорией по темам: «Способы проникновения вредоносных программ в систему», «Социальная инженерия», «Технологии внедрения», осуществляется через модуль «Занятия». Дискуссия проводится по темам: «Одновременное использование технологий внедрения и методов социальной инженерии», «Противодействие антивирусным программам», организованны через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – представлен алгоритм проверки ПО антивирусом.

Тема 2.2. Исполняемые файлы и расширения вредоносных кодов. – 2 ч.

Знакомство обучающихся с теорией по теме: «Правила Кибергигиены», «50 потенциально опасных расширений в Windows», через модуль «Занятия» Обсуждение тем: «Программы», «Скрипты», «Ярлыки», «Макросы» в режиме реального времени, посредством вебинара, организованного через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – составление презентации.

Тема 2.3. Вредоносная рассылка. – 2 ч.

Знакомство с теорией «Спам - что это такое?», «Понятие и виды спама», «Спам по категориям», путём размещения ссылок на теоретический материал в модуле «Занятия». Беседа на темы: «Способы распространения спама», «Борьба со спамом», организуется через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – составление презентации.

Тема 2.4. Вредоносные скрипты. – 2 ч.

Посредством просмотра видеоурока «Как проверить сайт на вирусы и вредоносные коды», ссылка на который размещена в модуле «Занятия». Обучающиеся принимают участие в обсуждении «О вредоносных скриптах: как они работают, чем опасны и как не столкнуться с ними», организованно через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – опрос.

Тема 2.5. Способы выявления наличия вредоносных кодов на устройствах. – 2 ч.

Знакомство с теоретическим материалом по темам: «Модель системы защиты от вредоносных программ», «Технический компонент», «Считывание файлов» и «Эмуляция», данный материал размещается на ресурсе «Занятия». На основе полученных данных в режиме видеоконсультации знакомятся с виртуализацией «песочница», проводят Мониторинг системных событий и поиск системных аномалий.
Форма контроля: осуществляется через модуль «Проверочные задания» – опрос.

Тема 2.6. Действия при обнаружении вредоносных кодов на устройствах. – 2 ч.

Изучение теоретического материала «Признаки заражения устройств вредоносными кодами», «Настройка параметров средств антивирусного контроля», материалы представлены в модуле «Занятия». Отработка алгоритма действий при возникновении инцидентов информационной безопасности, организованно через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – Составление

рекомендаций по защите информации от воздействия вредоносных кодов.

Раздел 3. Методы защиты от вредоносных программ. - 6 часов.

Тема 3.1. Способы защиты устройств от вредоносного кода. – 2 ч.

Ознакомление с теоретическим материалом «Защита информации от вредоносных программ», представленной в электронном виде в модуле «Занятия». Практическая работа над коллективным учебным проектом: «Можно ли защитить информацию?», организованно через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – предоставить фотографии работ по проекту «Можно ли защитить информацию?»

Тема 3.2. Антивирусные программы и их характеристики. – 2 ч.

Знакомство с основными антивирусными программами: «Антивирусные сканеры», «Мониторы (антивирусные сторожа)», «Полифаги», «Ревизоры», «Блокировщики», путём размещения информации в модуле «Занятия». Обсуждение изученных программ и принципов их действия, организуется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – опрос

Тема 3.3. Правила защиты от вредоносных кодов. – 2 ч.

Просмотр видео урока «Защита компьютерных систем от вредоносных программ», ссылка на видео размещена в описании урока модуля «Занятия». Дискуссия с обсуждением вопросов: Основные виды вредоносных программ, признаки заражения компьютера и способы защиты, - освоение через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – выполнение творческой работы по созданию буклета.

Раздел 4. Распространение вредоносного кода для мобильных устройств. – 4 часа.

Тема 4.1. Расширение вредоносных кодов для мобильных устройств. – 2 ч.

Знакомство с типами распространенных мобильных угроз, Имеющиеся на рынке средства защиты от мобильных угроз, а также эффективные личные тактики для снижения рисков компрометации мобильных устройств, освоение через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – опрос

Тема 4.2. Правила безопасности при установке приложений на мобильные устройства. – 2 ч.

Изучение статьи «Как НЕ скачать зловредное приложение для Android», размещение информации в модуле «Занятия». Беседа на тему: «Как безопасно пользоваться смартфоном, планшетом», освоение через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – выполнение творческой работы по созданию буклета.

Раздел 5. Выполнение и защита индивидуальных и групповых проектов. – 6 часов.

Тема 5.1. Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. – 1 ч.

Актуализация знаний по организации проектной деятельности, основными этапами разработки проектов и их назначением, организуется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – составление паспорта проекта

Тема 5.2. Цели, задачи, работа над проектом. Защита проекта. – 4 ч.

Изучение теоретического материала по теме, организуется через ссылку на теоретический материал.

Выделение проблемы, постановка целей и задач исследования. Формулировка гипотезы. Освоение методики исследования. Сбор собственного материала. Обработка собранного материала. Обобщение, анализ, выводы. Представление исследовательской работы, консультация по подготовке проекта осуществляется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – представление проектной папки.

Тема 5.3. Итоговое занятие. – 1 ч.

Подведение итогов года, видео встреча организуется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – выставка фотографий проектных работ.

Содержание программы 3 года обучения

Раздел 1. Социальная инженерия: распознать и избежать. – 9 часов.

Тема 1.1. Введение в программу. - 1 ч.

Актуализация знаний по организации рабочего места и правилами ТБ. Разберемся в понятиях: «Информационная безопасность», «Информационная грамотность», «Информационный иммунитет», «Медиаграмотность», через изучение презентации «Информационная безопасность» организованных через модули «Занятия» и «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – составление кроссворда «Информационная безопасность».

Тема 1.2. Приемы социальной инженерии. – 4 ч.

Знакомство с теорией, размещённой в модуле «Занятия»: «Что такое социальная инженерия?» «Виды атак с использованием социальной инженерии». Беседа и обсуждение вопросов: «Как избежать атаки с использованием социальной инженерии?», «Защита мобильных устройств» - через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – подготовить памятку «Как защитить свой телефон».

Тема 1.3. Правила безопасности в виртуальных контактах. – 4 ч.

Познакомиться с понятиями «Виртуальная реальность» и «Социальные сети», с правилами ответственного и безопасного поведения в современной информационной среде, размещение теоретического материала в модуле «Занятия» Обсуждение тем: «Причины и необходимость Интернет-общения, «Положительные и отрицательные стороны использования компьютера в повседневной жизни», Разработка рекомендаций, повышающих информированность населения о безопасном использовании онлайн-технологий; «Реальная и виртуальная дружба», через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – подготовить памятку «Правила безопасного общения в сети Интернет»

Раздел 2. Ложная информация в сети Интернет. - 5 часов.

Тема 2.1. Фейковые новости. – 3 ч.

Изучение статьи «Как распознать фейковые новости», размещенной в модуле «Занятия»**,** обсуждение изученного посредством ВКС, организованной через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – опрос

Тема 2.2. Поддельные страницы. – 2 ч.

Изучить теоретический материал с целью применения распознавать потенциально опасные схемы, которые могут использовать злоумышленники, чтобы украсть аккаунт или получить доступ к персональным данным, посредством модуля «Занятия». Познакомить обучающихся с понятиями «Дипфейк» и «Доксинг» — повысить уровень осведомленности о мошеннических схемах с использованием дипфейк технологий и определить спектр возможностей применения технологии дипфейк - путём просмотра видео урока «Как отличить настоящий сайт или страницу от подделки»

Форма контроля: осуществляется через модуль «Проверочные задания» – опрос

Раздел 3. Безопасность при использовании платежных карт в Интернете. – 6 часов.

Тема 3.1. Транзакции и связанные с ними риски. – 2 ч.
Знакомство с информацией: «Какие бывают транзакции?», «Как проводят транзакции?», «Когда могут отклонить транзакцию?» - просмотр видео урока «Как работают БАНКОВСКИЕ КАРТЫ?» - освоение через модуль «Занятия».
Форма контроля: осуществляется через модуль «Проверочные задания» – опрос
Тема 3.2. Правила совершения онлайн покупок. – 2 ч.
Рассмотреть возможные действия мошенников, направленные на хищение денежных средств, при совершении интернет покупки. Расширить и систематизировать представление школьников о персональных данных, в том числе о персональных данных банковской карты, способах защиты своих персональных данных и своих денежных средств. Изучение статьи «Правила безопасности при покупках в Интернете», - освоение через модуль «Занятия», путём размещения теоретических данных. Дискуссия на пройденную тему посредством ГИС «Навигатор» через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – опрос
Тема 3.3. Безопасность банковских сервисов. – 2 ч.
Изучение статьи «Пятнадцать правил безопасного использования банковских карт онлайн», размещённой в модуле «Занятия». Обсуждение вопросов: Что такое онлайн-банкинг? Преимущества онлайн-банкинга, Недостатки онлайн-банкинга, Риски онлайн-банкинга, Как защитить банковский счет от мошенников, освоение через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – подготовить Памятку «Безопасные покупки»

Раздел 4. Беспроводная технология связи. – 5 часов.
Тема 4.1. Уязвимости Wi-Fi-соединений. – 1 ч.
Изучение теории по теме: «Wi-Fi - беспроводная технология», «Основные угрозы безопасности», «Пентест», «Поддельная точка доступа», «MITM», «Атаки на протоколы WEP и WPA», «Ddos или Dos атаки» - через модуль «Занятия».
Форма контроля: осуществляется через модуль «Проверочные задания» – опрос
Тема 4.2. Публичные и непубличные сети. – 2 ч.
Изучение статьи «Облачные сети и подсети: частные и публичные, общие и клиентские», размещённой в модуле «Занятия». Обсуждение вопросов: «Канал связи», «Компьютерные сети», «Пропускная способность канала», «Локальная компьютерная сеть», «Глобальная компьютерная сеть» - через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – опрос
Тема 4.3. Правила работы в публичных сетях. – 2 ч.
Изучение 8 основных правил общения в сети Интернет, посредством модуля «Занятия» Дискуссия по вопросам: Что такое сетевой этикет? Что такое нетикет? -освоение через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – подготовить Памятку «Правила работы в публичных сетях»

Раздел 5. Резервное копирование данных. – 5 часов.
Тема 5.1. Безопасность личной информации. – 2 ч.
Ознакомление с материалами статьи «Кибербезопасность: как защитить личные данные в сети» - ссылка на статью в модуле «Занятия». Обсуждение тем: «Специальные персональные данные», «Биометрические персональные данные», «Набор цифр как персональные данные», «Кибербуллинг или киберзапугивание», «Изучение политики конфиденциальности», - освоение через модуль «Вебинары».
Форма контроля: осуществляется через модуль «Проверочные задания» – тест
Тема 5.2. Создание резервных копий на различных устройствах. – 3 ч.
Просмотр видео урока «Резервное копирование Windows. Создание и восстановление бэкапа», ссылка на видеоматериал в модуле «Занятия».Обсуждение тем и отработка

практических навыков: «Что из себя представляет система резервного копирования?», «Меры безопасности», «Установка системы резервного копирования», «Создание резервных копий на внешних жестких дисках по расписанию», «Необходимые шаги для настройки автоматического создания плановых резервных копий на внешних жестких дисках», «Создание резервных копий на DVD-дисках в ручном режиме для восстановления разделов или системы», «Восстановление файлов и папок», «Восстановление операционной системы» - через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – тест

Раздел 6. Выполнение и защита индивидуальных и групповых проектов. – 5 часов.

Тема 6.1. Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. – 1 ч.

Актуализация знаний по организации проектной деятельности, основными этапами разработки проектов и их назначением, организуется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – составление паспорта проекта

Тема 6.2. Цели, задачи, работа над проектом. Защита проекта. – 4 ч.

Изучение теоретического материала по теме, организуется через ссылку на теоретический материал.

Выделение проблемы, постановка целей и задач исследования. Формулировка гипотезы. Освоение методики исследования. Сбор собственного материала. Обработка собранного материала. Обобщение, анализ, выводы. Представление исследовательской работы, консультация по подготовке проекта осуществляется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – представление проектной папки.

Тема 6.3. Итоговое занятие. – 1 ч.

Подведение итогов года, видео встреча организуется через модуль «Вебинары».

Форма контроля: осуществляется через модуль «Проверочные задания» – выставка фотографий проектных работ.

Контрольно-оценочные средства

Результативность освоения дополнительной общеобразовательной программы «Информационная безопасность» определяется с помощью входного, текущего и итогового контроля.

Цель **входного контроля** – диагностика имеющихся знаний и умений обучающихся, общая эрудиция, ценностные ориентации.

Текущий контроль применяется для оценки качества освоения текущегоматериала по разделам и темам программы.

Формы оценки: творческие задания, проекты, создание интернет статей, видео роликов, выполнение презентаций и составление памяток и кроссвордов.

Итоговый контроль применяется для контроля выполнения поставленных задач.

Формы оценки: защита мини-проектов, итогового проекта, тестирование.

Контроль и оценка уровня образовательных результатов освоения дополнительной общеобразовательной программы «Информационная безопасность» осуществляется педагогом в процессе проведения занятий.

В конце учебного года педагог обобщает результаты всех диагностических процедур и определяет уровень результатов образовательной деятельности каждого обучающегося – интегрированный показатель, в котором отображена концентрация достижений всех этапов и составляющих учебно-воспитательного процесса. Возможные уровни освоения ребенком образовательных результатов по программе - низкий (Н), средний (С), высокий (В).

Мониторинг определения уровня образовательных результатов

Показатели (оцениваемые параметры)	Критерии	Степень выраженности оцениваемого качества	Кол-во баллов
Теоретическая подготовка ребенка:			
Теоретические знания (по основным разделам учебно-тематического плана программы)	Соответствие теоретических знаний ребенка программным требованиям	- *минимальный уровень* (ребенок овладел менее чем ½ объема знаний, предусмотренных программой); - *средний уровень* (объем усвоенных знаний составляет более ½); -*максимальный уровень* (ребенок освоил практически весь объем знаний, предусмотренных программой за конкретный период);	1 5 10
Владение специальной терминологией по тематике программы	Осмысленность и правильность использования специальной терминологии	- *минимальный уровень* (ребенок, как правило, избегает употреблять специальные термины); - *средний уровень* (ребенок сочетает специальную терминологию с бытовой); - *максимальный уровень* (специальные термины употребляет осознанно и в полном соответствии с их содержанием).	1 5 10
Практическая подготовка ребенка:			
Практические умения и навыки, предусмотренные программой (по основным разделам учебно-тематического плана программы)	Соответствие практических умений и навыков программным требованиям	- *минимальный уровень* (ребенок овладел менее чем ½ предусмотренных умений и навыков); - *средний уровень* (объем усвоенных умений и навыков составляет более ½); - *максимальный уровень* (ребенок овладел практически всеми умениями и навыками, предусмотренными программой за конкретный период);	1 5 10
Владение специальным оборудованием и оснащением	Отсутствие затруднений в использовании специального оборудования и оснащения	- *минимальный уровень умений* (ребенок испытывает серьезные затруднения при работе с оборудованием); - *средний уровень* (работает с оборудованием с помощью педагога); - *максимальный уровень* (работает с оборудованием самостоятельно, не испытывает особых трудностей);	1 5 10
Творческие навыки	Креативность в	- *начальный* (элементарный) уровень	1

(творческое отношение к делу и умение воплотить его в готовом продукте)	выполнении заданий	развития креативности (ребенок в состоянии выполнять лишь простейшие практические задания педагога); - *репродуктивный уровень* (выполняет в основном задания на основе образца); - *творческий уровень* (выполняет практические задания с элементами творчества).	 5 10
Общеучебные умения и навыки ребенка:			
Умение подбирать и анализировать специальную литературу	Самостоятельность в подборе и анализе литературе	- *минимальный уровень умений* (обучающийся испытывает серьезные затруднения при работе с литературой, нуждается в постоянной помощи и контроле педагога); - *средний уровень* (работает с литературой с помощью педагога или родителей); - *максимальный уровень* (работает с литературой самостоятельно, не испытывает особых трудностей)	1 5 10
Умение пользоваться компьютерными источниками информации	Самостоятельность в пользовании компьютерными источниками информации	уровни – по аналогии с вышеуказанными	
Умение осуществлять учебно-исследовательскую работу	Самостоятельность в учебно-исследовательской работе	уровни – по аналогии с вышеуказанными	
Умение слушать и слышать педагога	Адекватность восприятия информации, идущей от педагога	уровни – по аналогии с вышеуказанными	
Умение выступать перед аудиторией	Свобода владения и подачи обучающимся подготовленной информации	уровни – по аналогии с вышеуказанными	
Умение вести полемику, участвовать в дискуссии	Самостоятельность в построении дискуссионного выступления, логика в построении доказательств	уровни – по аналогии с вышеуказанными	
Умение организовать свое рабочее (учебное) место	Способность самостоятельно готовить свое рабочее	уровни – по аналогии с вышеуказанными	

	место к деятельности и убирать его за собой		
Навыки соблюдения в процессе деятельности правил безопасности	Соответствие реальных навыков соблюдения правил безопасности программным требованиям	- *минимальный уровень (*ребенок овладел менее чем ½ объема навыков соблюдения правил безопасности, предусмотренных программой); - *средний уровень* (объем усвоенных навыков составляет более ½); - *максимальный уровень* (ребенок освоил практически весь объем навыков, предусмотренных программой за конкретный период).	1 5 10
Умение аккуратно выполнять работу	Аккуратность и ответственность в работе	удовлетворительно – хорошо – отлично	

Условия реализации программы 1 года обучения

№	Название раздела	Учебно-методическое обеспечение	Кадровое обеспечение	Материально-техническое обеспечение	Информационно-образовательные ресурсы
1	Общение в социальных сетях и мессенджерах	Учебник теория социальных сетей,В.А. Чвякин, А.С. Чертков http://scipro.ru/conf/socialnetworks23.pdf	Педагог дополнительного образования, обладающий необходимыми компетенциями для реализации программы данной направленности.	Компьютер/ноутбук с доступом к сети интернет и доступ к ГИС «Навигатор дополнительного образования детей Омской области», модуль «Вебинары»	Рассказываем про технологии онлайн-коммуникаций https://vk.com/video-174311295_456239405 Тренажёр «Мессенжеры» на платформе «Урок Цифры» https://урокцифры.рф/lessons/messenger Основные форматы контента **https://practicum.yandex.ru/blog/osnovnye-vidy-kontenta/#formaty-kontenta**

2	С кем безопасно общаться в интернете	Статья «Сетевой этикет» https://www.kaspersky.ru/resource-center/preemptive-safety/what-is-netiquette			статья «Создаем пользовательский профиль» https://ux-journal.ru/bazovyj-kurs-ux-sozdanie-polzovatelskih-profilej.html Практическая работа «Управление профилями пользователей» контент- платформа https://pandia.ru/text/78/213/92463.php
3	Методы защиты от вредоносных программ	Python 3 для начинающих. Самоучитель. – URL: https://pythonworld.ru/samouchitel-python Демидова, М. «Генераторы Python: что это такое и зачем они нужны/М.Демидова – URL: https://skillbox.ru/media/code/generatory_python_chto_eto_takoe_i_zachem_oni_nuzhny/ Правила создания, использования и хранения паролей https://sbersova.ru/academy/courses/password/task/c44b8 Стоит ли сохранять пароли в браузере? https://www.kaspersky.ru/blog/how-to-store-passwords-securely/35876/			Как сделать брошюру через Google Документы – https://ru.wikihow.com/сделать-брошюру-через-Google Документы Создание буклета в Publisher – https://lumpics.ru/how-to-make-a-booklet- in-publisher/
4	Безопасный вход в аккаунты	Молдовян А.А., Молдовян Д.Н., Левина А.Б. Протоколы аутентификации с нулевым разглашением секрета.– https://books.ifmo.ru/file/pdf/1887.pdf			Как сохранить свой аккаунт? видео https://youtu.be/d9UP1bk0EdM
5	Настройки конфиденциальности в социальных сетях	Настройки безопасности и конфиденциальности Лекция 10: Безопасность в социальных сетях https://intuit.ru/studies/courses/3462/704/lecture/19435?page=2			"Приватность в социальной сети" видеоролик https://youtu.be/YJ1ERIYpl_s

6	Публикация информации в социальных сетях	Методическое пособие по работе в социальных сетях https://clib.yar.ru/wp-content/uploads/2018/10/SMM.pdf **"Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 23.03.2024) (с изм. и доп., вступ. в силу с 01.04.2024)**			Статья https://www.consultant.ru/document/cons_doc_LAW_10699/4234a27af714cc608ea71b7bae9400f3613c8f60/
7	Кибербуллинг	Методический сборник «ПРОкаждого: травля – это не норма» https://sdorus.ru/wp-content/uploads/2022/12/profilaktika_bullinga_metodicheskiy_sbornik.pdf			
8	Публичные аккаунты	Информационная безопасность 1.8 Публичные аккаунты https://it32mgn.ru/ib_1_8/			Видео урок «Приватность в соц.сетях https://www.youtube.com/watch?v=YJ1ERIYpl_s тренжер «Приватность в цифровом мире» https://урокцифры.рф/lessons/cybersecurity Обучающий видеоурок - Публичные и приватные страницы https://youtu.be/tBZdEsn3q24
9	Фишинг	Информационная безопасность 1.9 Фишинг https://it32mgn.ru/ib_1_9/ Статья «Что такое фишинг и как от него защититься» https://skillbox.ru/media/code/chto-takoe-fishing-i-kak-ot-nego-zashchititsya/			Видео урок «Социальные сети, мессенджеры и почтовые сервисы. Фейки и фишинг » https://youtu.be/vWOip_55wHA
10	Выполнение и защита индивидуальных и групповых проектов	Методические рекомендации учащимся по выполнению проектных и исследовательских работ https://sch842zg.mskobr.ru/files/metodicheskie_rekomendacii_proekty.pdf			Темы проектов https://it32mgn.ru/ib/

Условия реализации программы 2 года обучения

№	Название раздела	Учебно-методическое обеспечение	Кадровое обеспечение	Материально-техническое обеспечение	Информационно-образовательные ресурсы
1	Что такое вредоносный код	Лекция 5: Программно-математическое воздействие. Вредоносные программы и их классификация **https://intuit.ru/studies/courses/3649/891/lecture/32328** Статья «Что такое вредоносный код?» https://www.kaspersky.ru/resource-center/definitions/malicious-code	Педагог дополнительного образования, обладающий необходимыми компетенциями для реализации программы данной направленности.	Компьютер/ноутбук с доступом к сети интернет и доступ к ГИС «Навигатор дополнительного образования детей Омской области», модуль «Вебинары»	Видео урок «Виды вредоносного программного обеспечения» https://youtu.be/aHD1LgAv6Gk Вредоносные программы https://youtu.be/qFtSWp4mSfU
2	Распространение вредоносного кода	Карасева Э.М., Рак О.В. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ учебное пособие https://csukz.ru/nir/nui/2019/Учебное%20пособие%20Карасевой%20Э.М.,%20Рак%20О.В..pdf			Статья https://www.kaspersky.ru/resource-center/preemptive-safety/avoid-android-malware Видео урок «Как проверить сайт на вирусы и вредоносные коды» https://youtu.be/x5Rdgq3I8hk
3	Методы защиты от вредоносных программ	Т.А. Маркина СРЕДСТВА ЗАЩИТЫ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И СЕТЕЙ https://books.ifmo.ru/file/pdf/2121.pdf			видео урок «ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ» https://youtu.be/c8EOdfNeu4o
4	Распространение вредоносного кода для мобильных устройств	Статья онлайн журнал «Вредоносный код на мобильных устройствах и способы защиты от него» https://npsod.ru/analytics/1313.html			Безопасность веб-приложений - Эльдар Заитов https://habr.com/ru/companies/yandex/articles/414821/ Статья «Как НЕ скачать зловредное приложение для Android» https://www.kaspersky.ru/blog/android-

					app-security/18718/
5	Выполнение и защита индивидуальных и групповых проектов	Методические рекомендации учащимся по выполнению проектных и исследовательских работ https://sch842zg.mskobr.ru/files/metodicheskie_rekomendacii_proekty.pdf			Темы проектов https://it32mgn.ru/ib/

Условия реализации программы 3 года обучения

№	Название раздела	Учебно-методическое обеспечение	Кадровое обеспечение	Материально-техническое обеспечение	Информационно-образовательные ресурсы
1	Социальная инженерия: распознать и избежать	Статья: Как работает социальная инженерия. И как этим пользуются мошенники? https://journal.tinkoff.ru/social-engineering/	Педагог дополнительного образования, обладающий необходимыми компетенциями для реализации программы данной направленности.	Компьютер/ноутбук с доступом к сети интернет и доступ к ГИС «Навигатор дополнительного образования детей Омской области», модуль «Вебинары»	Видео СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ МОШЕННИКОВ https://youtu.be/0e68IePXL6U
2	Ложная информация в Интернете	Статья МАНИПУЛЯЦИИ В ИНТЕРНЕТЕ: ФЕЙКИ, ЛОЖЬ, НЕДОСТОВЕРНАЯ ИНФОРМАЦИЯ Что такое «фейк»? https://shkola16obninsk-r40.gosweb.gosuslugi.ru/netcat_files/30/69/Pamyatka_vzroslye_Feyki.pdf			Статья «Как распознать фейковые новости» https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-identify-fake-news видео урок «Как отличить настоящий сайт или страницу от подделки.» https://youtu.be/snSYcejU4VU

3	Безопасность при использовании платежных карт в Интернете	Статья «Правила безопасности при покупках в Интернете», https://moscowdebt.mos.ru/financial-gramotnost/rules-of-safety-when-shopping-online/index.php Сборник рекомендаций и памяток по безопасному использованию банковских карт и системы Интернет-банк https://apkbank.ru/common/upload/documents/Sbornik_rekomendatsiy_i_pamyatok_po_bezopasnomu_isp-u_bk_i_sist_IB_s_25.12.2023_sayt_stend_.pdf			Видео урок «Как работают БАНКОВСКИЕ КАРТЫ?» https://youtu.be/5j78f78H_Ig статья «Пятнадцать правил безопасного использования банковских карт онлайн» https://www.sberbank.ru/ru/person/kibrary/articles/pyatnadcat-pravil-bezopasnogo-ispolzovaniya-bankovskikh-kart-onlajn
4	Беспроводная технология связи	В.В. Жилин ТЕХНОЛОГИИ БЕСПРОВОДНОГО ДОСТУПА В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ https://cchgeu.ru/upload/iblock/3b2/gf5rvupdb2f06t31efvn239hx2h72dhu/TBDTS18.pdf			Статья «Облачные сети и подсети: частные и публичные, общие и клиентские» https://1cloud.ru/blog/publichnost-podseti
5	Резервное копирование данных	Статья 4.7. Резервное копирование данных https://studfile.net/preview/16568135/page:24/			Видео урок «Резервное копирование Windows. Создание и восстановление бэкапа» https://youtu.be/rHg_kV5xJnk Статья «КИБЕРБЕЗОПАСНОСТЬ: КАК ЗАЩИТИТЬ ЛИЧНЫЕ ДАННЫЕ В СЕТИ» https://media.foxford.ru/articles/kak-zashhitit-lichnye-dannye-v-seti

6	Выполнение и защита индивидуальных и групповых проектов	Методические рекомендации учащимся по выполнению проектных и исследовательских работ https://sch842zg.mskobr.ru/files/metodicheskie_rekomendacii_proekty.pdf			Темы проектов https://it32mgn.ru/ib/

Список литературы

Нормативные правовые документы

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации (с изменениями и дополнениями, вступившими в силу с 17.02.2023)
2. Распоряжение Правительства РФ от 31.03.2022 г. № 678-р «Об утверждении Концепции развития дополнительного образования детей до 2030 г. и плана мероприятий по ее реализации»
3. Приказ Минпросвещения России от 27.07.2022 № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»
4. Постановление Главного государственного санитарного врача РФ от 28.09.2020 № 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодёжи»

Список литературы для педагога

1. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. – Москва: ДМК Пресс, 2020. – 476 с.
2. Внуков, А. А. Основы информационной безопасности: защита информации / А. А. Внуков. – Москва: Юрайт, 2022. – 161 с.
3. Демидова М., Генераторы Python: что это такое и зачем они нужны. URL: https://skillbox.ru/media/code/generatory_python_chto_eto_takoe_i_zachem_oni_nuzhny/
4. Жилин, В.В., Технологии беспроводного доступа в телекоммуникационных системах: учеб. Пособие / В.В. Жилин. - Воронеж: ФГБОУ ВО «Воронежский государственный технический университет», 2018. – 112 с.
5. Жилин, В.В. Сравнительная характеристика современного антивирусного программного обеспечения / В.В. Жилин, Е.В. Палеха. – Москва: «Интернаука», 2017 – 239-246 с.
6. Карасева, Э.М., Рак, О.В. Основы информационной безопасности: Учебное пособие /Э.М. Карасева, О.В. Рак. – Костанайский филиал «ЧелГУ», Костанай, 2019. – 90 с.
7. Маркина, Т.А., Средства защиты вычислительных систем и сетей / Т.А. Маркина. – Санкт-Петербург: Университет ИТМО, 2016. – 72 с.
8. Мэйволд, Эрик. Безопасность сетей: самоучитель Шаг за шагом / Эрик Мэйволд. - Москва: Интуит, 2016. - 527 с.
9. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. – Санкт-Петербург: Лань, 2020. – 324 с.
8. Сборник рекомендаций и памяток по безопасному использованию банковских карт и системы интернет-банк. АО КБ "Агропромкредит", 2023.
9. Чвякин, В.А., Чертков А.С., Теория социальных сетей / В.А. Чвякин, А.С. Чертков. – Нижний Новгород: НОО Профессиональная наука, 2023. – 115 с.
10. Python 3 для начинающих. Самоучитель. URL: https://pythonworld.ru/samouchitel-

python

Список литературы для обучающихся и родителей:

1. Емельянова, Н.З. Защита информации в персональном компьютере / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – Москва: Форум, 2017. – 352 с.

2. Жук, А.П. Защита информации / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – Москва: Риор, 2017. – 480 с.

3. Камский, В. Защита личной информации в интернете, смартфоне и компьютере / В. Камский. – Санкт-Петербург: Наука и техника, 2017. – 272 с.

4. Колисниченко, Д.Н. Анонимность и безопасность в интернете. От «чайника» к пользователю / Д.Н. Колисниченко. – Санкт-Петербург: БХВ-Петербург, 2018. – 240 с.

5. Мазаник, С. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей / С. Мазаник. – Москва: Эксмо, 2019. – 256 с.

6. Мэйволд, Эрик. Безопасность сетей: самоучитель Шаг за шагом / Эрик Мэйволд. - Москва: Интуит, 2016. - 527 с.

Электронные образовательные ресурсы:

1. Блог Касперского - URL: https://www.kaspersky.ru/blog/ (дата обращения: 20.04.2024).

2. Урок Цифры — всероссийский образовательный проект в сфере цифровой экономики - URL: https://урокцифры.рф/(дата обращения: 20.04.2024).

3. Центр безопасного Интернета в России - URL: https://www.saferunet.ru/ (дата обращения: 20.04.2024).

4. Российская государственная детская библиотека- URL: https://rgdb.ru/ (дата обращения: 20.04.2024).