Муниципальное автономное общеобразовательное учреждение
Белоярского района «Средняя общеобразовательная школа № 3 г. Белоярский»

Рассмотрена на заседании
педагогического совета школы
Протокол от 16.12.2024 года № 6

Утверждена приказом
СОШ №3 г. Белоярский
от 16.12.2024 года № 840

Дополнительная общеобразовательная общеразвивающая программа технической направленности «Информационная безопасность. Кибербезопасность»

Возраст обучающихся: 15-18 лет
Срок реализации: 1 год

Автор-составитель:
Тутынина Ирина Анатольевна,
учитель информатики

Белоярский, 2024

Пояснительная записка

Дополнительная общеобразовательная общеразвивающая программа «Информационная безопасность. Кибербезопасность» (далее – программа) имеет техническую направленность и разработана для воспитания технически грамотной и творческой личности, а также формирования у обучающихся устойчивого интереса к деятельности, направленной на получение и применение новых знаний для решения технологических, инженерных, творческих, исследовательских и прикладных задач. Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма.

В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

Новизна программы заключается в использовании современных педагогических технологий, приемов; различных техник и способов работы; современного оборудования, позволяющего исследовать и моделировать различные объекты и системы из области нейротехнологий и машинного обучения. Программа адаптирована для старшего возраста обучающихся, собирающихся осуществлять исследовательскую, проектную и инженерную деятельность.

Актуальность и необходимость данной программы продиктована совершенствованием школьного образования и подготовки в сфере информационных технологий, а также популяризация профессий, связанных с информационными технологиями.

Педагогическая целесообразность программы - ориентация учащихся на техническое творчество, дальнейшее применение полученных начальных знаний, умений и навыков в научно-технических кружках, во время обучения в учреждениях среднего профессионального и высшего образования.

Государство считает необходимым расширение объема преподавания информационных технологий в общеобразовательных организациях. В качестве одной из организационных мер в обеспечении кибербезопасности определена разработка и внедрение в учебный процесс образовательных организаций разного уровня курса по информационной безопасности, включающего модули по обеспечению кибербезопасности, либо дополнение имеющихся курсов упомянутыми модулями. Школьная программа должна соответствовать этим целям, поэтому представляется актуальным реализация программы внеурочной деятельности «Основы кибербезопасности».

В основе отрасли кибербезопасности лежит формирование на качественно новом уровне культуры умственного труда и взаимодействия с окружающими, ответственного отношения к вопросам безопасности жизнедеятельности.

Данная программа состоит из 7 модулей:

- Общие сведения о безопасности ПК и Интернета
- Техника безопасности и экология
- Проблемы Интернет-зависимости
- Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы
- Мошеннические действия в Интернете. Киберпреступления
- Сетевой этикет. Психология и сеть
- Правовые аспекты защиты киберпространства

Отличительная особенность программы состоит в освоении трёх типов содержания:

мировоззренческого, знаниевого и деятельностного. В области мировоззрения программа предполагает переход от ценности потребления к развитию, далее – к развитию науки. В области знания предполагается расширение имеющегося знания до современного предметного знания, далее – работа в проблемных, открытых естественнонаучных областях и смежных науках.

В деятельности предлагается применять полученные информационные знания в практических сферах и проектах, что особенно важно при анализе при работе на стыке нескольких предметов.

Направленность программы – техническая.

Уровень освоения программы – базовый. Формирование и развитие творческих способностей детей, формирование общей культуры учащихся; удовлетворение индивидуальных потребностей в интеллектуальном, нравственном и физическом совершенствовании, формирование культуры здорового и безопасного образа жизни, укрепление здоровья, а также на организацию их свободного времени.

Целевая аудитория

Характеристики обучающихся, возрастные особенности, иные медико-психолого-педагогические характеристики

Программа рассчитана на обучение и развитие обучающихся 15-18лет. Подростка отличает стремление к самостоятельности, независимости, к самопознанию, формируются познавательные интересы. Задача педагога доверять подростку решение посильных для него вопросов, уважать его мнение. Общение предпочтительнее строить не в форме прямых распоряжений и назиданий, а в форме проблемных вопросов. У подростка появляется умение ставить перед собой и решать задачи, самостоятельно мыслить и трудиться. Подросток проявляет инициативу, желание реализовать и утвердить себя. В этот период происходит окончательное формирование интеллекта, совершенствуется способность к абстрактному мышлению. Для старшего подростка становится потребностью быть взрослым. Проявляется стремление к самоутверждению себя в роли взрослого.

Задача педагога побуждать обучающегося к открытию себя как личности и индивидуальности в контексте художественного творчества, к самопознанию, самоопределению и самореализации. Совместная деятельность для школьников этого возраста привлекательна как пространство для общения. Для возрастной категории 15-18 лет при решении кейсов и разработке проектов предусмотрены задания повышенного уровня сложности, применяется оборудование, соответствующее возрасту. В программе запланировано проведение комбинированных (смешанных) занятий: занятия состоят из теоретической и практической частей, причём большее количество времени занимает именно практическая часть. Это связано с тем, что основная цель программы состоит в том, чтобы дать обучающемуся как можно больше практических знаний и сформировать как можно больше практических умений.

Форма обучения: очная, очная с применением дистанционных технологий.

Особенности организации образовательного процесса

Учащиеся организуются в учебную группу постоянного состава. Формы занятий: групповые (10-15 человек). Отбор содержания основан на принципах научности, доступности, преемственности, практической направленности, учитывает возрастные особенности учащихся.

Практические занятия будут направлены на решение расчетных и практических задач. Создание мини-проекта предполагает знакомство с технологией ведения проектной деятельности. На занятиях ученик будет попробовать себя в специфических видах деятельности, присущих информатики (планирование, проведение эксперимента и обработка полученных результатов, решение более сложных расчетных, экспериментальных и качественных задач). При организации занятий предусматривается использование следующих методов и видов обучения:

1) словесный метод выражается в разъяснениях заданий, непонятных моментов, в рассказах о примерах проявлений изучаемых явлений в нашей жизни и практике, в больших лекциях по углублению уже полученных знаний, в дискуссиях по вопросам занятий;
2) наглядный метод в демонстрации программ процессов, и т.д.;
3) практический метод реализуется безопасном поведении при работе с компьютерными программами, информацией в сети интернет
4) частично-поисковый, исследовательский метод - через выполнение мини-проекта и выполнения практических задания.

Программа основана на следующих принципах: доступности, наглядности, системности, последовательности.

Для подготовки к выступлениям, соревнованиям могут быть объединены обучающиеся разных групп.

Содержание программы предусматривает развитие творческих способностей детей, формирование начальных информационных знаний, навыков, умений, способствует приобретению чувства уверенности и успешности, психологического благополучия, навыков разбиения задачи на подзадачи, работы в команде, ведения мозгового штурма, применения логического и аналитического мышлений, навыков по работе с современными программами в области информационных технологий и машинного обучения.

Сроки освоения программы и её объём

Программа рассчитана на 1 год обучения, объём программы 72 часа.

Цель программы – создание условий для формирования у учащихся цифровой культуры личности с необходимыми навыками и присущими ценностями, взглядами, ориентациями, установками, мотивами деятельности и поведения для обеспечения безопасной и развивающей жизнедеятельности учащегося в сети «Интернет».

Задачи программы:

Обучающие:

- Сформировать систему знаний в сфере обществознания, информационных технологий и основ безопасности жизнедеятельности;
- Обучить элементам системного мышления использовать инструменты активизации мышления;
- Отработка навыков и умений для безопасного и полезного использования информационных технологий: сравнение информации, критический анализ, выделение главных мыслей и грамотное изложение, а также восприятия и усвоения информации из сети «Интернет».

Развивающие:

- Развить интеллектуальные и социальные способности обучающихся;
- Развить навыки сетевого общения и коммуникации в сети «Интернет», поиска и работы с информацией, обеспечения безопасности цифровых устройств и аккаунтов и осуществления сетевых покупок;
- Развить деловые и гражданские качества, такие как самостоятельность, ответственность, активность и аккуратность;
- Сформировать потребности в самопознании и саморазвитии.
- Стимулировать познавательную активность обучающихся посредством включения их в различные виды конкурсной деятельности;
- Формировать ключевые компетенции обучающихся.

Воспитательные:

- Воспитать культуру общения и поведения в сетевом пространстве;
- Воспитать целеустремлённость личности;
- Воспитать толерантную и культурную личность;
- Воспитывать дисциплинированность, ответственность, самоорганизацию;
- Воспитать трудолюбие, уважение к труду;

- Формировать чувство коллективизма и взаимопомощи;
- Способствовать раскрытию внутреннего мира обучающихся;
- Формировать новаторское отношение ко всем сферам жизнедеятельности человека;
- Воспитывать самостоятельность в приобретении дополнительных знаний и умений;
- Воспитывать дисциплинированность, ответственность, самоорганизацию;
- Воспитать трудолюбие, уважение к труду;
- Формировать чувство коллективизма и взаимопомощи;
- Способствовать раскрытию внутреннего мира обучающихся;
- Формировать новаторское отношение ко всем сферам жизнедеятельности человека;
- Воспитывать самостоятельность в приобретении дополнительных знаний и умений;
- Воспитывать чувство патриотизма, гражданственности, гордости за достижения отечественной науки и техники.

Принципы реализации программы:

- системность, целостность, объективность, научность, доступность для обучающихся, реалистичность, практическая направленность;
- комплексность и взаимосвязь всех факторов, влияющих на процесс воспитания;
- единство восприятия, обучения, развития;
- сочетание педагогического руководства с развитием активности, самостоятельности и инициативы учащихся;
- системность и последовательность образования и воспитания;
- учет возрастных индивидуальных особенностей обучающегося

Формы реализации программы

Программа реализуется в очной форме. В целях оказания содействия лицам, которые проявили выдающиеся способности, показавшим высокий уровень интеллектуального развития и творческих способностей возможна организация образовательного процесса по индивидуальному учебному плану. В ходе реализации программы применяются различные современные образовательные технологии Курс «Профессия — Белый Хакер»", https://stepik.org/course/127 — курс по аудиту безопасности веб-проектов от Mail.ru Group. Будет полезен тем, кто только начинает изучать категорию web), в том числе дистанционные образовательные технологии, электронное обучение; предпочтение отдается активным формам и методам обучения (экскурсии, подготовка и защита творческих проектов, интеллектуальные игры, круглые столы и т.д.), вместе с тем осуществляются и традиционные формы образовательной деятельности (эвристическая беседа, лекции, практические работы и т.д.).

Результаты обучения:

- Защита творческих проектов, обучающихся;
- Участие в конкурсах;
- Публикации обучающихся;
- Мониторинг учебных достижений, обучающихся;
- Отчеты по практическим, экспериментальным работам обучающихся;
- Защита исследовательских работ.

Прогнозируемый результат освоения программы

должны знать:

- О безопасном поведении при работе с компьютерными программами, информацией в сети интернет;
- Нормы информационной этики;
- Правила поиска и отбора информации, её интерпретации и применимости
- Безопасное и полезное использование информационных технологий: сравнение информации, критический анализ, выделение главных мыслей и грамотное изложение, а также восприятия и усвоения информации из сети «Интернет»

Должны уметь:

- Соблюдать технику безопасности;
- Разбивать задачи на подзадачи;
- Работать в команде;
- Проводить мозговой штурм;
- Применять логическое и аналитическое мышление при решении задач.

УЧЕБНЫЙ ПЛАН

№ п/п	Наименование модулей	Кол-во часов
1	Общие сведения о безопасности ПК и Интернета	10
2	Техника безопасности и экология.	7
3	Проблемы Интернет-зависимости	5
4	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	24
5	Мошеннические действия в Интернете. Киберпреступления	8
6	Сетевой этикет. Психология и сеть	11
7	Правовые аспекты защиты киберпространства	7
	Всего часов:	**72**

Модуль 1. Общие сведения о безопасности ПК и Интернета (10 часов).

Как работают мобильные устройства. Угрозы для мобильных устройств.

Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр).

Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации).

Кто обеспечивает защиту киберпространства.

Что такое геоинформационные системы (ГИС). Глобальные информационные Сети по стихийным бедствиям.

Модуль 2. Техника безопасности и экология (7 часов).

Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности.

Компьютеры и мобильные устройства в экстремальных условиях.

Везде ли есть Интернет. ТБ при работе с мобильными устройствами.

Первая помощь при проблемах в интернете (службы помощи).

Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).

Модуль 3. Проблемы Интернет-зависимости (5 часов).

Виды Интернет-зависимости.

Компьютер и зрение.

Модуль 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (24 часа).

Вирусы и антивирусы.

Как распространяются вирусы.

Источники и причины заражения.

Скорая компьютерная помощь. Признаки заражения компьютера.

Что такое антивирусная защита. Как лечить компьютер.

Защита мобильных устройств.

Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.

Защита файлов. Что такое право доступа.

Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления (8 часов).

Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС.

Прослушивание разговоров. Определение местоположения телефона.

Модуль 6. Сетевой этикет. Психология и сеть (11 часов).

Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.

«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам.

Анонимность в сети.

Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.

Как появился не этикет, что это такое. Общие правила сетевого этикета.

Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).

Этика дискуссий. Взаимное уважение при интернет-общении.

Этикет и безопасность. Эмоции в сети, их выражение.

Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.

Если вы стали жертвой компьютерной агрессии: службы помощи.

Модуль 7. Правовые аспекты защиты киберпространства (7 чаов).

Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация.

Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».

Учебно-тематический план

№ урока	Тема	Кол-во часов
	Общие сведения о безопасности ПК и Интернета	**10**
1	Как работают мобильные устройства. Угрозы для мобильных устройств.	1
2	Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр).	1
3	Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации).	1
4	Кто обеспечивает защиту киберпространства.	1
5	Что такое геоинформационные системы (ГИС). Глобальные информационные Сети по стихийным бедствиям.	1
6	Информационная безопасность	1
7	Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные.	1
8	Источники данных в Интернете: почта, сервисы обмена файлами и	1

	др. Хранение данных в Интернете.	
9	Возможности и проблемы социальных сетей.	1
10	Безопасный профиль в социальных сетях. Составление сети контактов.	1
	Техника безопасности и экология.	**7**
11	Комплекс упражнений при работе за компьютером.	**1**
12	Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов	**1**
13	Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности.	1
14	Компьютеры и мобильные устройства в экстремальных условиях.	1
15	Везде ли есть Интернет. ТБ при работе с мобильными устройствами.	1
16	Первая помощь при проблемах в интернете (службы помощи).	1
17	Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).	1
	Проблемы Интернет-зависимости.	**5**
18	Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред.	**1**
19	Киберкультура (массовая культура в сети) и личность.	**1**
20	Психологическое воздействие информации на человека. Управление личностью через сеть.	**1**
21	Виды Интернет-зависимости.	1
22	Компьютер и зрение.	1
	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	**24**
23	Как распространяются вирусы.	1
24	Источники и причины заражения.	1
25	Скорая компьютерная помощь. Признаки заражения компьютера.	1
26	Что такое антивирусная защита. Как лечить компьютер.	1
27	Защита мобильных устройств.	1
28	Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.	1
29	Защита файлов. Что такое право доступа.	1
30	Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.	1
31	Защита файлов. Права пользователей.	1
32	Защита при загрузке и выключении компьютера.	1
33	Безопасность при скачивании файлов.	1
34	Безопасность при просмотре фильмов онлайн.	1
35	Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты.	1
36	Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы.	1
37	Методы защиты фото и видеоматериалов от копирования в сети.	1
38	Защита от копирования контента сайта.	1
39	Как развивались вирусы.	1
40	Могут ли вирусы воздействовать на аппаратуру ПК.	1
41	Как вирусы воздействуют на файлы.	1

42	Проверка на наличие вирусов. Сканеры и др.	1
43	Может ли вирус воздействовать на рабочий стол.	1
44	Источники заражения ПК.	1
45	Антивирусное ПО, виды и назначение.	1
46	Методы защиты от вирусов. Как распознаются вирусы.	1
	Мошеннические действия в Интернете. Киберпреступления.	**8**
47-48	Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС.	2
49-50	Прослушивание разговоров. Определение местоположения телефона.	2
51	Утечка и обнародование личных данных.	1
52	Подбор и перехват паролей. Взломы аккаунтов в социальных сетях.	1
53	Виды мошенничества в Интернете. Фишинг (фарминг).	1
54	Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею.	1
	Сетевой этикет. Психология и сеть.	**11**
55	Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.	1
56	«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам.	1
57	Анонимность в сети.	1
58	Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.	1
59	Как появился нетикет, что это такое. Общие правила сетевого этикета.	1
60	Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).	1
61	Этика дискуссий. Взаимное уважение при интернет-общении.	1
62	Этикет и безопасность. Эмоции в сети, их выражение.	1
63	Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.	1
64	Если вы стали жертвой компьютерной агрессии: службы помощи.	1
65	Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид	1
	Правовые аспекты защиты киберпространства.	**7**
66-67	Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация.	2
68	Защита прав потребителей при использовании услуг Интернет.	1
69	Защита прав потребителей услуг провайдера.	1
70-72	Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	3

Календарный учебный график

№ урока	Дата	Время проведения	Тема	Кол-во	Форма занятия

				часов	
			Общие сведения о безопасности ПК и Интернета	**10**	
1			Как работают мобильные устройства. Угрозы для мобильных устройств.	1	лекция
2			Распространение вредоносных файлов через приложения для смартфонов и планшетов (скачивание фотографий, музыки, игр).	1	лекция
3			Виды защиты киберпространства (что такое несанкционированный доступ, разрушение и утрата информации, искажение информации).	1	Дискуссии
4			Кто обеспечивает защиту киберпространства.	1	Практическое занятие
5			Что такое геоинформационные системы (ГИС). Глобальные информационные Сети по стихийным бедствиям.	1	Презентация
6			Информационная безопасность	1	Презентация Дискуссии
7			Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные.	1	Лекции
8			Источники данных в Интернете: почта, сервисы обмена файлами и др. Хранение данных в Интернете.	1	Практическое занятие
9			Возможности и проблемы социальных сетей.	1	Лекции
10			Безопасный профиль в социальных сетях. Составление сети контактов.	1	Презентация Практическое занятие
			Техника безопасности и экология.	**7**	
11			Комплекс упражнений при работе за компьютером.	**1**	Практическое занятие
12			Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов	**1**	Практическое занятие
13			Компьютер и мобильные устройства в чрезвычайных ситуациях. Дополнения к ДТП. Компьютер и мобильные (сотовые) устройства в правилах безопасности.	1	Презентация
14			Компьютеры и мобильные устройства в экстремальных условиях.	1	Практическое занятие
15			Везде ли есть Интернет. ТБ при работе с мобильными устройствами.	1	Практическое занятие
16			Первая помощь при проблемах в интернете (службы помощи).	1	Семинар коллоквиумы
17			Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).	1	Практическое занятие
			Проблемы Интернет-зависимости.	**5**	

18			Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред.	**1**	Практическое занятие
19			Киберкультура (массовая культура в сети) и личность.	**1**	Защита проекта
20			Психологическое воздействие информации на человека. Управление личностью через сеть.	**1**	Практическое занятие
21			Виды Интернет-зависимости.	1	Практическое занятие
22			Компьютер и зрение.	1	Презентация
			Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	**24**	
23			Как распространяются вирусы.	1	Презентация
24			Источники и причины заражения.	1	Презентация Дискуссии
25			Скорая компьютерная помощь. Признаки заражения компьютера.	1	Лекции
26			Что такое антивирусная защита. Как лечить компьютер.	1	Практическое занятие
27			Защита мобильных устройств.	1	Лекции
28			Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.	1	Презентация Практическое занятие
29			Защита файлов. Что такое право доступа.	1	Презентация
30			Защита детей в социальных сетях. ПО для родителей. Ограничение времени нахождения в сети.	1	Практическое занятие
31			Защита файлов. Права пользователей.	1	Практическое занятие
32			Защита при загрузке и выключении компьютера.	1	Презентация
33			Безопасность при скачивании файлов.	1	Практическое занятие
34			Безопасность при просмотре фильмов онлайн.	1	Практическое занятие
35			Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты.	1	Семинар коллоквиумы
36			Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Неперемещаемые программы.	1	Практическое занятие

37			Методы защиты фото и видеоматериалов от копирования в сети.	1	Конференция
38			Защита от копирования контента сайта.	1	Практическое занятие
39			Как развивались вирусы.	1	Защита проекта
40			Могут ли вирусы воздействовать на аппаратуру ПК.	1	Практическое занятие
41			Как вирусы воздействуют на файлы.	1	Практическое занятие
42			Проверка на наличие вирусов. Сканеры и др.	1	Презентация
43			Может ли вирус воздействовать на рабочий стол.	1	Практическое занятие
44			Источники заражения ПК.	1	Практическое занятие
45			Антивирусное ПО, виды и назначение.	1	Семинар коллоквиумы
46			Методы защиты от вирусов. Как распознаются вирусы.	1	Практическое занятие
			Мошеннические действия в Интернете. Киберпреступления.	**8**	
47-48			Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС.	2	Практическое занятие
49-50			Прослушивание разговоров. Определение местоположения телефона.	2	Защита проекта
51			Утечка и обнародование личных данных.	1	Практическое занятие
52			Подбор и перехват паролей. Взломы аккаунтов в социальных сетях.	1	Практическое занятие
53			Виды мошенничества в Интернете. Фишинг (фарминг).	1	Презентация
54			Азартные игры. Онлайн-казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею.	1	Практическое занятие
			Сетевой этикет. Психология и сеть.	**11**	
55			Что такое личные данные. Все, что выложено в Интернет, может стать известно всем.	1	Презентация
56			«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам.	1	Практическое занятие
57			Анонимность в сети.	1	Практическое занятие
58			Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.	1	Семинар коллоквиумы

59			Как появился нетикет, что это такое. Общие правила сетевого этикета.	1	Практическое занятие
60			Личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).	1	Конференция
61			Этика дискуссий. Взаимное уважение при интернет-общении.	1	Практическое занятие
62			Этикет и безопасность. Эмоции в сети, их выражение.	1	Презентация
63			Реальная и виртуальная личность, реальные встречи с виртуальными знакомыми и их опасность, угрозы и оскорбления – чем это может закончиться.	1	Практическое занятие
64			Если вы стали жертвой компьютерной агрессии: службы помощи.	1	Практическое занятие
65			Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид	1	Семинар коллоквиумы
			Правовые аспекты защиты киберпространства.	**7**	
66-67			Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация.	2	Практическое занятие
68			Защита прав потребителей при использовании услуг Интернет.	1	Семинар коллоквиумы
69			Защита прав потребителей услуг провайдера.	1	Практическое занятие
70-72			Обобщение материала курса. Игра-квест «Знатоки кибербезопасности».	3	Защита проекта

Методические материалы

Данная программа одновременно формирует у учащихся языковую и научно-исследовательскую компетентность, предполагает изучение теоретического материала и

выполнение практических заданий, способствующих усвоению и закреплению умений и навыков использования различной информации для формирования собственного мнения и прогнозирования деятельности. При выполнении практических заданий, помогающих раскрыть основные теоретические положения, необходимо подвести итог, сделать самостоятельный вывод о значении информационной безопасности во время занятий. Система занятий по данной программе включает дискуссии, в ходе которых перед обучающимися ставятся исследовательские задачи, что способствует формированию соответствующих умений, развитию высокого уровня активности, воспитанию личностного отношения к содержанию обучения в дистанционном обучении. Процесс обучения построен на принципе «от простого к сложному», с учетом возрастных особенностей обучающихся, доступности материала, развивающего обучения.

Виды контроля:

- вводный, который проводится перед началом работы и предназначен для закрепления знаний, умений и навыков по пройденным темам;
- текущий, проводимый в ходе занятия и закрепляющий знания поданной теме;
- итоговый, проводимый после завершения всей программы.

Формы проверки результатов:

- наблюдение за обучающимися в процессе работы;
- соревнования;
- индивидуальные и коллективные исследовательские проекты.

Формы подведения итогов:

- выполнение практических заданий (тесты) и лабораторных работ;
- творческое задание (подготовка проекта и его презентация).

Качество реализации программы отслеживается при помощи мониторинга результативности образовательной деятельности обучаемого, ориентированного на задачи программы.

Цель мониторинга: проверить и проанализировать сформированность следующих показателей:

1. Уровень усвоения теоретического материала и его практическое применение.
2. Стремление к самообразованию.
3. Способность формулировать и излагать свое мнение.
4. Ответственное отношение к выполнению проекта.

Критерии оценивания:

Уровень ниже заданного – практически не прослеживается освоение теоретического материала и качество выполнения практических заданий, не стремиться к самообразованию, не умеет формулировать и излагать свое мнение; не принимает участие в групповом проекте.

Низкий уровень – слабо прослеживается освоение теоретического материала и качество выполнения практических заданий, стремление к самообразованию, не уверенно формулирует и излагает свое мнение; практически не

принимает участие в групповом проекте.

Средний уровень – удовлетворительно (достаточно хорошо) прослеживается освоение теоретического материала и качество выполнения практических заданий, стремление к самообразованию, хорошо формулирует и излагает свое мнение; принимает участие в групповом проекте.

Высокий уровень – хорошо прослеживается освоение теоретического материала и качество выполнения практических заданий, стремление к самообразованию, отлично формулирует и излагает свое мнение; активно принимает участие в групповом проекте.

Уровень ниже заданного – 0, низкий уровень – 1, средний уровень – 2, высокий уровень – 3.

Для отслеживания и фиксации образовательных результатов используются:

- портфолио;
- фотоматериалы;

- материалы анкетирования и тестирования.

Портфолио является наиболее наглядной формой отслеживания и фиксации результатов. Портфолио включает общие сведения об учащемся, реферативное описание результативности работы в кружке, грамоты, дипломы, сертификаты о победах и участии в различных мероприятиях (конкурсах, выставках, соревнованиях), продукты деятельности (распечатку презентаций проектов и сами проекты), информацию, подтверждающую участие обучающегося в конкурсах и конференциях.

Защита портфолио является формой итоговой аттестации. Другими формами предъявления результатов деятельности обучающихся объединения служат:

Методы обучения по программе:

В методике приводится следующая классификация методов обучения: Пассивные: когда учитель доминирует, а учащиеся — пассивны. Такие методы используются на отдельных занятиях обучающего типа. Самый распространенный прием пассивных методов — лекция. Активные. Здесь учитель и ученик выступают как равноправные участники урока, взаимодействие происходит по вектору учитель = ученик. Интерактивные — наиболее эффективные методы, при которых ученики взаимодействуют не только с учителем, но и друг с другом. Вектор: учитель = ученик= ученик. Метод проектов предполагает самостоятельный анализ заданной ситуации и умение находить решение проблемы. Проблемный метод предполагает постановку проблемы (проблемной ситуации, проблемного вопроса) и поиск решений этой проблемы через анализ подобных ситуаций (вопросов, явлений).Эвристический метод объединяет разнообразные игровые приемы в форме конкурсов, деловых и ролевых игр, соревнований, исследований. Исследовательский метод перекликается с проблемным методом обучения. Только здесь учитель сам формулирует проблему. Задача учеников — организовать исследовательскую работу по изучению проблемы.

Педагогические технологии:

При реализации программы используются следующие педагогические технологии:

- технология группового обучения - для организации совместных действий, коммуникаций, общения, взаимопонимания и взаимопомощи;

- технология дифференцированного обучения – применяются задания различной сложности в зависимости от интеллектуальной подготовки учащихся;

- технология эдьютеймент – для воссоздания и усвоения обучающимися изучаемого материала, общественного опыта и образовательной деятельности;

- технология проблемного обучения – для творческого усвоения знаний, поэтапного формирования умственных действий, активизации различных операциймышления;

- технология проектной деятельности - для развития исследовательских умений; достижения определенной цели; решения познавательных и практических задач; приобретения коммуникативных умений при работе в группах;

- информационно-коммуникационные технологии – применяются для расширения знаний, выполнения заданий, создания и демонстрации презентаций назанятиях, проведения диагностики и самодиагностики.

Примерная тематика докладов и проектных работ:

1. Кибербезопасность, как защититься от киберугроз.
2. Кибербезопасность – виды мошенничества и защита от мошенников.
3. Кибербезопасность и искусственный интеллект.
4. Кибербезопасность школьника.
5. Новые подходы к обеспечению кибербезопасности, выявление уязвимостей в современных системах.
6. Актуальные угрозы в области кибербезопасности.
7. Современные методы защиты информации от киберугроз.
8. Способы атак на информационные системы
9. Методы защиты. Шифрование данных
10. Искусственный интеллект в кибербезопасности
11. Блокчейн в защите информации.

12. Цифровая гигиена.
13. Текущие тенденции и угрозы в области информационной безопасности.
14.

Список использованной литературы

1. Закон РФ «Об образовании в РФ».

Методические материалы

2. Тонких И.М., Комаров М.М., Ледовской В.И., Михайлов А.В. Основы кибербезопасности, Москва, 2016
3. Stepik.org: Курс «Профессия — Белый Хакер» (https://stepik.org/course/169003/promo)
4. https://stepik.org/course/127 — курс по аудиту безопасности веб-проектов от Mail.ru Group. Будет полезен тем, кто только начинает изучать категорию web
5. Портал Международного квеста по цифровой грамотности www.Сетевичок.рф
https://toipkro.ru/content/files/documents/podrazdeleniya/ordo/ciber%20bezopasnost.pdf