Департамент образования и науки Брянской области
Государственное автономное учреждение дополнительного образования
«Центр цифрового образования «АЙТИ-куб» Дятьковского района»

Рассмотрено на заседании
методического совета
Протокол № 1
от «28» августа 2024

Принято решением
педагогического совета
Протокол № 1
от «30» августа 2024

УТВЕРЖДАЮ
Директор ГАУ ДО «Центр цифрового образования «АЙТИ-куб»
Дятьковского района»
Приказ № 77-о/д от «30» августа 2024

ДОКУМЕНТ ПОДПИСАН
УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00C7ACEA5257F95783EAAB798F4E880F7B
Владелец: Короткова Елена Николаевна
Действителен: с 06.03.24г. 9:43:33 по 30.05.25г. 9:43:33

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ (ОБЩЕРАЗВИВАЮЩАЯ) ПРОГРАММА

технической направленности

«Цифровая гигиена и работа с большими данными»

возраст обучающихся: 9-11 лет, срок реализации: 1 год

Автор-составитель:
Дудкина Нина Петровна,
Исаева Марина Александровна,
педагоги дополнительного образования

г. Дятьково, 2024

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеобразовательная (общеразвивающая) программа «Цифровая гигиена и работа с большими данными» (далее - Программа), разработана в соответствии с нормативно-правовыми основаниями:

- Федеральным Законом №273-ФЗ от 29.12.2012 г. «Об образовании в Российской Федерации»;
- Указом Президента Российской Федерации «О национальных целях развития Российской Федерации на период до 2030 года»;
- Конвенцией развития дополнительного образования детей до 2030 года (утверждена распоряжением Правительства РФ от 31.03.2022 г. №678-р);
- Стратегией развития воспитания в Российской Федерации на период до 2025 года (утверждена распоряжением Правительства Российской Федерации от 29.05.2015 г. № 996-р);
- Планом мероприятий по реализации в 2021 – 2025 годах Стратегии развития воспитания в Российской Федерации на период до 2025 года (утвержден распоряжением Правительства Российской Федерации от 12.11.2020 г. № 2945-р);
- Приказом Министерства образования и науки Российской Федерации от 23.08.2017 г. №816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;
- Приказом Министерства просвещения Российской Федерации от 27.07.2022 г. №629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
- Приказом Министерства просвещения Российской Федерации от 03.09.2019 г. № 467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей»;

- Постановлением Главного государственного санитарного врача РФ от 28.09.2020 г. №28 «Об утверждении СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи»»;
- Письмом Министерства образования и науки Российской Федерации от 18.11.2015 г. №09-3242 «О направлении информации» (с «Методическими рекомендациями по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы))»;
- Конвенцией ООН о правах ребёнка.

Направленность программы

Программа «Цифровая гигиена и работа с большими данными» имеет техническую направленность. Данная направленность ориентирована на создание условий для вовлечения детей в создание искусственно- технических и виртуальных объектов, построенных по законам природы, в приобретение навыков в области обработки материалов, электротехники и электроники, системной инженерии, 3D-прототипирования, цифровизации, работы с большими данными, освоения языков программирования, машинного обучения, автоматизации и робототехники, технологического предпринимательства, содействовать формированию у обучающихся современных знаний, умений и навыков в области технических наук, технологической грамотности и инженерного мышления и предназначена для использования в системе дополнительного образования детей.

Сущность программы «Цифровая гигиена и работа с большими данными» целенаправлена на обучение детей навыкам безопасного поведения в всемирной сети Internet, защите персональных данных, приватности в онлайн-среде и работе с большими данными. Также ребята освоят Microsoft Office. Знание офисных программ позволит свободно создавать, оформлять, редактировать текстовые документы, работать с электронными таблицами, создавать презентации. Эти знания пригодятся не только для учебы, но и для любой сферы деятельности.

Актуальность

В настоящее время выросла потребность общества в технически грамотных специалистах, полностью отвечающих социальному заказу по подготовке квалифицированных кадров в области кибергигиены. Данная программа строится на концепции подготовки обучающихся к профессии киберследователя – профессии будущего, выделенной в «Атласе новых профессий» (проект «Агентства стратегических инициатив» по исследованию рынка труда, 2015 г.) и предполагающей проведение расследований киберпреступлений посредством поиска информации и обработки информации в интернет-пространстве.

Программа актуальна тем, что не имеет аналогов на рынке общеобразовательных услуг и является своего рода уникальным образовательным продуктом в области информационных технологий. Знания, умения и навыки решения актуальных задач, полученные на занятиях, готовят обучающихся к самостоятельной проектно-исследовательской деятельности с применением современных технологий.

Новизна или отличительные особенности

Отличительной особенностью программы «Цифровая гигиена и работа с большими данными» является её фокус на решение практических задач. Это означает, что в рамках обучения воспитанники обучаются не только теоретическим знаниям в области кибербезопасности, но и получают опыт и навыки по реальным примерам с использованием современных технологий. В программе изучается полный пакет прикладных программ для обработки информации. Освоение программы происходит в основном в процессе практической творческой деятельности.

Педагогическая целесообразность

Данная программа педагогически целесообразна, так как ее реализация органично вписывается в единое образовательное пространство данной образовательной организации. Программа соответствует новым стандартам

обучения, которые обладают отличительной особенностью, способствующей личностному росту учащихся, его социализации и адаптации в обществе.

Программа «Цифровая гигиена и работа с большими данными» является целостной и непрерывной в течение всего процесса обучения. Развивает навыки исследовательской деятельности и анализа информации в интернет-пространстве, обнаружения источников информации.

При изучении данной Программы обучающиеся научатся распознавать опасный и вредоносный контент, манипулирование сознанием и внушение потенциально опасных идей в интернет-пространстве. Полученные знания и умения позволят критически оценивать и классифицировать получаемую в интернет-пространстве информацию, использовать ее в положительных целях и нейтрализовать ее негативное влияние.

Цель Программы

Целью Программы является получение навыков работы с большими данными, развитие творческих способностей у обучающихся к комплексному анализу информации, размещенной на различных интернет-ресурсах в интересах безопасного и рационального использования интернет пространства, формирование информационной культуры, а также подготовка обучающихся, как компетентных пользователей, умеющих работать с современными компьютерными технологиями для решения пользовательских, учебных и профессиональных задач.

Задачи Программы

Обучающие:

- формирование о структуре и типах информации в интернет-пространстве, больших данных;
- формирование общекультурных навыки работы с информацией;
- ознакомление с методами и средствами поиска информации в интернет-пространстве;
- ознакомление обучающихся с основами исследовательской деятельности;

- формирование навыка планирования, проведения и обработки результатов исследования информации в интернет-пространстве при помощи поисковых систем, общедоступных средств поиска информации и системы мониторинга и анализа социальных медиа «Крибрум»;
- формирование способности определять социальные характеристики и индивидуальные особенности людей и обнаруживать признаки опасного поведения на основании их аккаунтов в социальных сетях;
- формирование умения работать с полным пакетом прикладных программ для обработки информации.

Развивающие:

- создание условий для развития поисковой активности, исследовательского решения;
- развитие самостоятельности и творческого подхода к решению задач;
- развитие логического, технического мышления;
- способствование к формированию умения практического применения полученных знаний;
- формирование у обучающихся способностей успешной самопрезентации и создания позитивного имиджа в социальных сетях;
- создание мотивации к постоянному самообразованию.

Воспитательные:

- развитие коммуникативной культуры обучающихся, как внутри проектных групп, так и в коллективе в целом;
- создание творческой атмосферы, обеспечивающей развитие личности, социализацию и эмоциональное благополучие каждого воспитанника;
- формирование информационной культуры;
- воспитание ценностного отношения к своему здоровью.

Адресат Программы

Возраст обучающихся, участвующих в реализации данной программы - от 9 до 11 лет.

Образовательный процесс осуществляются в группах с обучающимися разного возраста. Программа предоставляет обучающимся возможность освоения учебного содержания занятий с учетом уровня их общего развития, способностей, мотивации. В рамках Программы предполагается реализация параллельных процессов освоения содержания Программы на разных уровнях доступности и степени сложности, с опорой на диагностику стартовых возможностей каждого из воспитанников.

В коллектив могут быть приняты все желающие, не имеющие противопоказаний по здоровью.

Количество обучающихся в одной группе варьируется от 8 до 12 человек.

Срок реализации Программы – 1 год (144 часа).

Формы обучения - сочетание очной и очно-заочной форм образования с применением электронного обучения и дистанционных образовательных технологий (Закон №273-ФЗ, гл.2, ст.17, п.2.).

Реализация Программы предполагает использование здоровьесберегающих технологий.

Занятия проводятся 2 раза в неделю по 2 академических часа. Продолжительность академического часа - 45 минут. После первой половины занятия организовывается перерыв 10 минут для проветривания помещения и отдыха обучающихся.

Планируемые результаты

Предметные результаты

Обучающийся будет:

- владеть основными приемами работы в прикладных программах для обработки информации;

- иметь представление о структуре и типах информации в интернет-пространстве, больших данных и больших пользовательских данных;
- понимать методы и средства поиска информации в интернет-пространстве;
- применять навыки планирования, проведения и обработки результатов исследования информации в интернет-пространстве при помощи поисковых систем, общедоступных средств поиска информации и системы мониторинга и анализа социальных медиа «Крибрум»;
- уметь выявлять и критически оценивать источники и каналы распространения информации в интернет-пространстве и определять ее качество;
- уметь определять социальные характеристики и индивидуальные особенности людей, обнаруживать признаки опасного поведения на основании их аккаунтов в социальных сетях;
- уметь распознавать опасный и вредный контент и идентифицировать явления манипулирования сознанием в интернет-пространстве, внушения деструктивных идей и вовлечения в социально опасные группы в социальных сетях.

Личностные результаты

У обучающегося будут сформированы:

- устойчивый интерес к правилам здоровье сберегающего и безопасного поведения;
- умения проявлять в самостоятельной деятельности логическую культуру и компетентность;
- аналитическое, практическое и логическое мышление;
- самостоятельность и самоорганизацию;
- умение работать в команде, развить коммуникативные навыки;
- умение вести себя сдержанно и спокойно.

Метапредметные результаты

Обучающийся научится:

- самостоятельно планировать последовательность своих действий для достижения поставленных целей, а также грамотно распределять свое время и ресурсы для получения максимально эффективного результата;
- организовать учебное сотрудничество и совместную деятельность с педагогом и сверстниками;
- продуктивно общаться и взаимодействовать в процессе совместной деятельности, учитывать позиции других участников деятельности, эффективно разрешать конфликты;
- принимать решений, а также умение формулировать, аргументировать и отстаивать своё мнение.

Формы аттестации и подведения итогов реализации дополнительной образовательной программы

Система отслеживания результатов обучающихся выстроена следующим образом:

- входной контроль (определение начального уровня знаний, умений и навыков);
- промежуточный контроль (промежуточная аттестация);
- итоговый контроль (итоговая аттестация).

Входной контроль по программе «Цифровая гигиена и работа с большими данными» проводится с целью выявления у обучающихся начальных представлений в области пользования компьютерной техникой и программным обеспечением, представлений о правилах безопасного взаимодействия с другими пользователями Интернета. Осуществляется по следующим параметрам:

- техника безопасности (навыки безопасного поведения, понимание инструкций по технике безопасности);
- мотивированность;

- зрелость (знание простейших понятий в области кибергигиены, умение выстраивать взаимодействие со сверстниками);
- умелость (элементарные навыки пользования ПК);
- владение терминологией (понимание сути и различий явлений в сети).

Входной контроль осуществляется самим педагогом в сентябре месяце на первых занятиях в свободной форме.

Промежуточная аттестация проводится в конце первого полугодия в декабре месяце. На усмотрении педагога промежуточный контроль может осуществляться в любой форме, например, в форме презентации работ, на которой обучающиеся демонстрируют уровень овладения теоретическим и практическим программным материалом или в виде интерактивного тестирования, где обучающиеся соревнуясь между собой отвечают на вопросы по теме (учитывается правильность и скорость ответов) и т.д.

Итоговая аттестация во втором полугодии (в конце каждого года обучения) - обязательно, в любой выбранной педагогом и обучающимся форме (прописанной в образовательной программе Центра). Как правило, итоговый контроль проходит в виде защиты индивидуальных/групповых проектов.

УЧЕБНЫЙ ПЛАН

№ п/п	Название раздела, темы	Общее кол-во часов	В том числе		Формы аттестации/ контроля
			Теория	Практика	
Введение		**2**	**1**	**1**	
1	Вводный инструктаж по ТБ. Знакомство с предметом	2	1	1	Опрос
Раздел 1. Изучение пакета прикладных программ для обработки информации		**24**	**6**	**18**	
2	Текстовые редакторы	6	1	5	Опрос, практическая работа
3	Презентации	6	2	4	
4	Электронные таблицы	6	2	4	
5	Графические редакторы	6	1	5	
Раздел 2. Безопасность общения		**24**	**8**	**16**	
6	Защита электронной почты	6	2	4	Опрос, практическая работа
7	Общение в социальных сетях и мессенджерах	6	2	4	
8	Конфиденциальность в социальных сетях	8	2	6	
9	Публикация информации в социальных сетях	4	2	2	
Раздел 3. Анализ мнений интернет-пользователей		**16**	**4**	**12**	
10	Информация в интернет-пространстве	4	2	2	Опрос, практическая работа
11	Поиск информации в системе «Крибрум»	6	1	5	
12	Анализ мнений об определенных темах	6	1	5	
Раздел 4. Распознавание опасного и вредного контента в интернет-пространстве		**14**	**4**	**10**	

№ п/п	Название раздела, темы	Общее кол-во часов	В том числе		Формы аттестации/ контроля
			Теория	Практика	
13	Опасные и вредный контент	6	2	4	Опрос, практическая работа
14	Противодействие угрозам интернет-пространства	8	2	6	
Раздел 5. Безопасность устройств и информации на них		**32**	**8**	**24**	
15	Беспроводная технология Связи	6	2	4	Опрос, практическая работа
16	Использование платежных карт в Интернете	8	2	6	
17	Кибербуллинг. Фишинг	10	2	8	
18	Резервное копирование	8	2	6	
Раздел 6. Порядок действий ликвидации последствий сбоев системы		**18**	**4**	**14**	
19	Кибератаки и сбои систем	6	2	4	Опрос, практическая работа
20	Вредоносные ПО	12	2	10	
Проектная деятельность		**14**	**2**	**12**	
21	Обобщение материала, разработка проектов	14	2	12	Проектная работа
Итого:		**144**	**37**	**107**	

СОДЕРЖАНИЕ ПРОГРАММЫ

Введение

Теория

Знакомство с работой творческого объединения, проведение инструкций по охране труда и техники безопасности. Входной контроль.

Раздел 1. Изучение пакета прикладных программ для обработки информации

Теория

Знакомство и работа с прикладными программами для обработки информации. Знакомство с текстовым редактором. Работа с клавиатурой в текстовом редакторе. Изучение программ создания презентаций и их возможностями. Правила составления презентации. Работа в программе с электронными таблицами, построение диаграмм. Изучение графических редакторов.

Практика

Работа с прикладными программами для обработки информации (текстовые редакторы, создание презентаций, работа с электронными таблицами и диаграммами). Работа в графических редакторах.

Раздел 2. Безопасность общения

Теория

Защита электронной почты, шифрование сообщений, с кем безопасно общаться, пароли для аккаунтов социальных сетей.

Практика

Настройка электронной почты для безопасного общения, работа с шифрование сообщений, настройки конфиденциальности в социальных сетях, подбор безопасных паролей для аккаунтов, изучение правил безопасных паролей, генератор паролей.

Раздел 3. Анализ мнений интернет-пользователей

Теория

Знакомство с методологией исследования информации в интернет-пространстве, сопоставление различных мнений по определенной теме и выявлять общие тенденции.

Практика

Работа с поиском информации в интернет пространстве при помощи системы «Крибрум». Создание презентации.

Раздел 4. Распознавание опасного и вредного контента в интернет-пространстве

Теория

Распознавание опасного контента (фишинг, мошенничество, вовлечение в опасные виды деятельности), определение источников и каналов распространения. Изучение противодействия угрозам интернет-пространства.

Практика

Учащиеся проанализируют распространение в социальных сетях объявления о сборе средств, конкурсах, акциях, продаже товаров, дарении, услугах экстрасенсов при помощи системы «Крибрум», а также проверят достоверность данных объявлений. В заключение учащиеся алгоритмизируют действия при столкновении с подозрительным контентом в интернете и представят их на интеллект-карте.

Раздел 5. Безопасность устройств и информации на них

Теория

Изучение технологии беспроводной технологии связи, безопасность личных данных при онлайн-оплате, изучение облачных хранилищ.

Практика

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях. Разработка возможных вариантов решения ситуаций, связанных с рисками использования платежных карт в Интернете. Создание резервных копий на различных устройствах.

Раздел 6. Порядок действий ликвидации последствий сбоев системы

Теория

Определение кибератак и сбои в системе. Анализ информации о способах защиты от вредоносного программного обеспечения. Изучение способов профилактики и лечения вирусов.

Практика

Учащиеся в этой теме оценят способы заражения компьютера с помощью сети Интернет.

Проектная деятельность

Теория

Самостоятельный выбор учащимися тем проектов, разработка плана работы для его реализации.

Практика

Подготовка плана работы для реализации программы, поиск информации, патентный поиск, побор литературы, подготовка работ для участия в различных конкурсах и мероприятиях.

УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Требования к помещению

Для обеспечения занятий необходимо:

- помещение, отвечающее санитарно-гигиеническим требованиям: просторное, с хорошим дневным освещением, хорошо налаженной вентиляцией;
- помещение должно быть оборудовано необходимой мебелью (столы, стулья, шкафы, доска, стеллажи);
- освещение может быть электрическое, лучи света должны падать на изображаемый объект под углом 45º;
- окна должны быть защищены от воздействия прямых солнечных лучей (занавес, жалюзи).

Материально-техническое обеспечение:

- ноутбук тип 1 (13 шт.);
- веб-камера (1 шт.);
- наушники с микрофоном (13 шт.);
- мышь (13 шт.);
- многофункциональное устройство (1 шт.);
- моноблочное интерактивное устройство (1 шт.);
- мобильная напольная стойка (1 шт.);
- флипчарт (1 шт.);
- стол ученический 2-местный (с экраном между столов) (6 шт.);
- стул ученический (12 шт.);
- стол преподавателя (1 шт.);
- шкаф (2 шт.);
- стул преподавателя (1 шт.).

Информационное обеспечение:

- операционная система (желательно Windows);

- поддерживаемые браузеры (для работы LMS): Yandex Browser, Chrome, Chrome Mobile, Firefox, Opera.

СПИСОК ЛИТЕРАТУРЫ

Нормативные документы:

1. Федеральным Законом №273-ФЗ от 29.12.2012 «Об образовании в Российской Федерации»;

2. Указом Президента Российской Федерации «О национальных целях развития Российской Федерации на период до 2030 года»;

3. Конвенцией развития дополнительного образования до 2030 года (утверждена распоряжением Правительства РФ от 31.03.2022 №678-р);

4. Стратегией развития воспитания в Российской Федерации на период до 2025 года (утверждена распоряжением Правительства Российской Федерации от 29.05.2015 № 996-р);

5. Планом мероприятий по реализации в 2021 – 2025 годах Стратегии развития воспитания в Российской Федерации на период до 2025 года (утвержден распоряжением Правительства Российской Федерации от 12.11.2020 г. № 2945-р);

6. Приказом Министерства образования и науки Российской Федерации от 23.08.2017 №816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

7. Приказом Министерства просвещения Российской Федерации от 27.07.2022 №629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

8. Приказом Министерства просвещения Российской Федерации от 03.09.2019 № 467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей»;

9. Постановлением Главного государственного санитарного врача РФ от 28.09.2020 №28 «Об утверждении СП 2.4.3648-20 «Санитарно-

эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи»»;

10. Письмом Министерства образования и науки Российской Федерации от 18.11.2015 №09-3242 «О направлении информации» (с «Методическими рекомендациями по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы))»;

11. Конвенцией ООН о правах ребёнка.

Учебная литература:

1. Ашманов И. С. Идеальный поиск в Интернете глазами пользователя. М.: Питер, 2011;

2. Богачева Т. Ю., Соболева А. Н., Соколова А. А. Риски интернет пространства для здоровья подростков и пути их минимизации // Наука для образования: Коллективная монография. М.: АНО «ЦНПРО», 2015;

3. Герцог Г.А. Основы научного исследования: методология, методика, практика: учебное пособие. Челябинск: Изд-во Челяб. гос. пед. ун та, 2013;

4. Гончаров М. В., Земсков А.И., Колосов К.А., Шрайберг Я.Л. Открытый доступ: зарубежный и отечественный опыт состояние и перспективы // Научные и технические библиотеки. 2012. № 8. С. 5-26;

5. Горошко Е. И. Современная Интернет-коммуникация: структура и основные параметры // Интернет-коммуникация как новая речевая формация: коллективная монография / науч. ред. Т. Н. Колокольцева, О. В. Лутовинова. М.: Флинта: Наука, 2012;

6. Ефимова Л. Л., Кочерга С.А. Информационная безопасность детей: российский и зарубежный опыт: Монография. М.: ЮНИТИ-ДАНА, 2013;

7. Кабани Ш. SMM в стиле дзен. Стань гуру продвижения в социальных сетях и новых медиа! М.: Питер, 2012;

8. Кравченко А.И. Методология и методы социологических исследований. Учебник. М.: Юрайт, 2015;

9. Машкова С. Г. Интернет-журналистика: учебное пособие. Тамбов: Изд-во ТГТУ, 2012;

10. Попов А. Блоги. Новая сфера влияния. М.: Манн, Иванов и Фербер, 2008;

11. Слугина Н. Активные пользователи социальных сетей Интернета. СПб.: Питер, 2013;

12. Солдатова Г., Зотова Е., Лебешева М., Вляпников В. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. Ч. 1. Лекции. М.: Google, 2013;

13. Солдатова Г.У., Шляпников В.Н., Журина М.А. Эволюция онлайн рисков: итоги пятилетней работы линии помощи «Дети онлайн» // Консультативная психология и психотерапия. 2015. № 3. С. 50-66;

14. Федоров А.В. Медиаобразование: вчера и сегодня. М: МОО ВПП ЮНЕСКО «Информация для всех», 2009;

15. Ших К. Эра Facebook. М.: Манн, Иванов и Фербер, 2011;

16. Щербаков А.Ю. Интернет-аналитика. Поиск и оценка информации в web-ресурсах. Практическое пособие. М.: Книжный мир, 2012.

Интернет-ресурсы:

1. Федеральный портал «Российское образование» [Электронный ресурс]. Режим доступа: http://www.edu.ru;

2. Международная федерация образования [Электронный ресурс]. – Режим доступа: http://www.mfo-rus.org;

3. Образование: национальный проект [Электронный ресурс]. – Режим доступа: http://www.rost.ru/projects/education/education_main.shtml;

4. Сайт министерства образования и науки РФ [Электронный ресурс]. – Режим доступа: http://www.mon.gov.ru;

5. Планета образования: проект [Электронный ресурс]. – Режим доступа: http://www.planetaedu.ru;

6. Российское школьное образование [Электронный ресурс]. – Режим доступа: http://www.school.edu.ru;

7. Портал «Дополнительное образование детей» [Электронный ресурс]. – Режим доступа: http://vidod.edu.ru;

8. Платформа «Крибрум» [Электронный ресурс]. – Режим доступа: https://my.kribrum.ru;

9. Публичный поиск «Крибрум» [Электронный ресурс]. – Режим доступа: https://brahms.kribrum.ru.

Приложение 1

Календарно-тематическое планирование

Группа – ЦГ1

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
	Введение	**2**	**1**	**1**		
1	Вводный инструктаж по ТБ. Входной контроль. Знакомство с предметом	2	1	1	02.09	
	Раздел 1. Изучение пакета прикладных программ для обработки информации	**24**	**6**	**18**		
2	Изучение текстовых редакторов. Изучение интерфейса	2	1	1	04.09	
3	Работа с клавиатурой в текстовом редакторе	2	0	2	09.09	
4	Работа в текстовом редакторе	2	0	2	11.09	
5	Презентации и из возможности. Правила созданий презентаций	2	1	1	16.09	
6	Работа с презентациями	2	1	1	18.09	
7	Создание презентаций определенной тематики	2	0	2	23.09	
8	Программы для работы с электронными таблицами	2	1	1	25.09	
9	Работа с электронными таблицами	2	0	2	30.09	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
10	Расчеты в электронных таблицах	2	1	1	02.10	
11	Изучение графических редакторов	2	1	1	07.10	
12	Работа в графическом редакторе	2	0	2	09.10	
13	Создание рисунков на свободную тему	2	0	2	14.10	
	Раздел 2. Безопасность общения	**24**	**8**	**16**		
14	Электронная почта, виды	2	1	1	16.10	
15	Правила защиты электронной почты	2	1	1	21.10	
16	Настройка шифрования в почтовых клиентах	2	0	2	23.10	
17	Социальная сеть. История социальных сетей. Мессенджеры	2	1	1	28. 10	
18	Правила добавления друзей в социальных сетях. Правила сетевого общения	2	1	1	30.10	
19	Анализ общения обучающихся в социальных сетях	2	0	2	06.11	
20	Профиль пользователя. Анонимные социальные сети	2	1	1	11.11	
21	Сложные пароли. Правила хранения паролей	2	1	1	13.11	
22	Настройки конфиденциальности в социальных сетях и мессенджерах	2	0	2	18.11	
23	Виды аутентификации. Настройки безопасности аккаунта	2	0	2	20.11	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
24	Публикация личной информации	2	1	1	25.11	
25	Правила ведения публичных страниц	2	1	1	27.11	
	Раздел 3. Анализ мнений интернет-пользователей	**16**	**4**	**12**		
26	Изучение платформы «Крибрум». Работа с информацией в системе	2	1	1	02.12	
27	Поиск информации в интернет-пространстве	2	1	1	04.12	
28	Поиск информации в системе «Крибрум»	2	0	2	09.12	
29	Работа с информацией в системе «Крибрум»	2	1	1	11.12	
30	Работа с данными исследований. Визуализация	2	0	2	16.12	
31	Обобщение информации из разных источников	2	0	2	18.12	
32	Использование методов отработки информации	2	0	2	23.12	
33	Описание результатов исследования в системе «Крибрум»	2	1	1	25.12	
	Раздел 4. Распознавание опасного и вредного контента в интернет-пространстве	**14**	**4**	**10**		
34	Промежуточная аттестация. Виды опасного контента и его распознавание	2	1	1	30.12	
35	Повторный инструктаж по ТБ. Мошенничество, опасные виды деятельности	2	0	2	13.01	
36	Определение каналов распространения опасного контента	2	1	1	15.01.	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
37	Анализ распространения информации о сборе средств, конкурсах, акциях, продажах в системе «Крибрум»	2	0	2	20.01	
38	Оказание поддельных услуг. Подозрительные объявления	2	1	1	22.01	
39	Основные признаки подозрительного контента	2	0	2	27.01	
40	Составление карты действий при столкновении подозрительным контентом	2	1	1	29.01	
	Раздел 5. Безопасность устройств и информации на них	**32**	**8**	**24**		
41	Беспроводная связь. Уязвимость Wi-Fi-соединений	2	1	1	03.02	
42	Публичные и непубличные сети	2	0	2	05.02	
43	Правила работы в публичных сетях	2	1	1	10.02	
44	Транзакции и связанные с ними риски	2	1	1	12.02	
45	Правила совершения онлайн покупок	2	1	1	17.02	
46	Обзор сайтов онлайн-продаж	2	0	2	19.02	
47	Безопасность банковских сервисов	2	0	2	24.02	
48	Определение кибербуллинга и его виды	2	1	1	26.02	
49	Причины кибербуллинга и его последствий	2	0	2	03.03	
50	Способы избавления от кибербуллинга. Помощь жертве кибербуллинга	2	0	2	05.03	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
51	Фишинг. Популярные варианты распространения фишинга	2	1	1	10.03	
52	Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах	2	0	2	12.03	
53	Виды облачных хранилищ. Сравнительный анализ	2	1	1	17.03	
54	Совместная работа с облачными сервисами	2	0	2	19.03	
55	Безопасность личной информации	2	1	1	24.03	
56	Создание резервных копий на различных устройствах	2	0	2	26.03	
	Раздел 6. Порядок действий ликвидации последствий сбоев системы	**18**	**4**	**14**		
57	Понятие сбоя системы и кибератаки и синего экрана	2	1	1	31.03	
58	Способы распространения и заражения	2	1	1	02.04	
59	Работа с восстановлением данных	2	0	2	07.04	
60	Кража персональных данных с помощью вредоносного ПО	2	1	1	09.04	
61	Способы доставки вредоносных кодов. Вредоносная рассылка	2	0	2	14.04	
62	Распространение вредоносного кода для мобильных устройств	2	0	2	16.04	
63	Способы распознавания вредоносных программ мобильных устройств	2	0	2	21.04	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
64	Способы защиты устройств от вредоносного кода	2	1	1	23.04	
65	Антивирусные программы	2	0	2	28.04	
	Проектная деятельность	**14**	**2**	**12**		
66	Выбор тематики итоговых проектов	2	0	2	30.04	
67	Анализ выбранной темы. Поиск информации.	2	0	2	05.05	
68	Проектная деятельность. Обработка информации.	2	0	2	07.05	
69	Проектная деятельность. Оформление проектов	2	0	2	12.05	
70	Проектная деятельность. Работа над проектом	2	1	1	14.05	
71	Проектная деятельность. Предзащита проектов	2	1	1	19.05	
72	Итоговая аттестация. Проектная деятельность. Защита проектов	2	0	2	21.05	
	Итого:	**144**	**37**	**107**		

Приложение 2

Группы – ЦГ2

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
	Введение	**2**	**1**	**1**		
1	Вводный инструктаж по ТБ. Входной контроль. Знакомство с предметом	2	1	1	03.09	
	Раздел 1. Изучение пакета прикладных программ для обработки информации	**24**	**6**	**18**		
2	Изучение текстовых редакторов. Изучение интерфейса	2	1	1	05.09	
3	Работа с клавиатурой в текстовом редакторе	2	0	2	10.09	
4	Работа в текстовом редакторе	2	0	2	12.09	
5	Презентации и из возможности. Правила созданий презентаций	2	1	1	17.09	
6	Работа с презентациями	2	1	1	19.09	
7	Создание презентаций определенной тематики	2	0	2	24.09	
8	Программы для работы с электронными таблицами	2	1	1	26.09	
9	Работа с электронными таблицами	2	0	2	01.10	
10	Расчеты в электронных таблицах	2	1	1	03.10	
11	Изучение графических редакторов	2	1	1	08.10	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
12	Работа в графическом редакторе	2	0	2	10.10	
13	Создание рисунков на свободную тему	2	0	2	15.10	
	Раздел 2. Безопасность общения	**24**	**8**	**16**		
14	Электронная почта, виды	2	1	1	17.10	
15	Правила защиты электронной почты	2	1	1	22.10	
16	Настройка шифрования в почтовых клиентах	2	0	2	24.10	
17	Социальная сеть. История социальных сетей. Мессенджеры	2	1	1	29.10	
18	Правила добавления друзей в социальных сетях. Правила сетевого общения	2	1	1	31.10	
19	Анализ общения обучающихся в социальных сетях	2	0	2	05.11	
20	Профиль пользователя. Анонимные социальные сети	2	1	1	07.11	
21	Сложные пароли. Правила хранения паролей	2	1	1	12.11	
22	Настройки конфиденциальности в социальных сетях и мессенджерах	2	0	2	14.11	
23	Виды аутентификации. Настройки безопасности аккаунта	2	0	2	19.11	
24	Публикация личной информации	2	1	1	21.11	
25	Правила ведения публичных страниц	2	1	1	26.11	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
	Раздел 3. Анализ мнений интернет-пользователей	**16**	**4**	**12**		
26	Изучение платформы «Крибрум». Работа с информацией в системе	2	1	1	28.11	
27	Поиск информации в интернет-пространстве	2	1	1	03.12	
28	Поиск информации в системе «Крибрум»	2	0	2	05.12	
29	Работа с информацией в системе «Крибрум»	2	1	1	10.12	
30	Работа с данными исследований. Визуализация	2	0	2	12.12	
31	Обобщение информации из разных источников	2	0	2	17.12	
32	Использование методов отработки информации	2	0	2	19.12	
33	Описание результатов исследования в системе «Крибрум»	2	1	1	24.12	
	Раздел 4. Распознавание опасного и вредного контента в интернет-пространстве	**14**	**4**	**10**		
34	Промежуточная аттестация. Виды опасного контента и его распознавание	2	1	1	26.12	
35	Повторный инструктаж по ТБ. Мошенничество, опасные виды деятельности	2	0	2	09.01	
36	Определение каналов распространения опасного контента	2	1	1	14.01	
37	Анализ распространения информации о сборе средств, конкурсах, акциях, продажах в системе «Крибрум»	2	0	2	16.01	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
38	Оказание поддельных услуг. Подозрительные объявления	2	1	1	21.01	
39	Основные признаки подозрительного контента	2	0	2	23.01	
40	Составление карты действий при столкновении подозрительным контентом	2	1	1	28.01	
	Раздел 5. Безопасность устройств и информации на них	**32**	**8**	**24**		
41	Беспроводная связь. Уязвимость Wi-Fi-соединений	2	1	1	30.01	
42	Публичные и непубличные сети	2	0	2	04.02	
43	Правила работы в публичных сетях	2	1	1	06.02	
44	Транзакции и связанные с ними риски	2	1	1	11.02	
45	Правила совершения онлайн покупок	2	1	1	13.02	
46	Обзор сайтов онлайн-продаж	2	0	2	18.02	
47	Безопасность банковских сервисов	2	0	2	20.02	
48	Определение кибербуллинга и его виды	2	1	1	25.02	
49	Причины кибербуллинга и его последствий	2	0	2	27.02	
50	Способы избавления от кибербуллинга. Помощь жертве кибербуллинга	2	0	2	04.03	
51	Фишинг. Популярные варианты распространения фишинга	2	1	1	06.03	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
52	Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах	2	0	2	11.03	
53	Виды облачных хранилищ. Сравнительный анализ	2	1	1	13.03	
54	Совместная работа с облачными сервисами	2	0	2	18.03	
55	Безопасность личной информации	2	1	1	20.03	
56	Создание резервных копий на различных устройствах	2	0	2	25.03	
	Раздел 6. Порядок действий ликвидации последствий сбоев системы	**18**	**4**	**14**		
57	Понятие сбоя системы и кибератаки и синего экрана	2	1	1	27.03	
58	Способы распространения и заражения	2	1	1	01.04	
59	Работа с восстановлением данных	2	0	2	03.04	
60	Кража персональных данных с помощью вредоносного ПО	2	1	1	08.04	
61	Способы доставки вредоносных кодов. Вредоносная рассылка	2	0	2	10.04	
62	Распространение вредоносного кода для мобильных устройств	2	0	2	15.04	
63	Способы распознавания вредоносных программ мобильных устройств	2	0	2	17.04	
64	Способы защиты устройств от вредоносного кода	2	1	1	22.04	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
65	Антивирусные программы	2	0	2	24.04	
	Проектная деятельность	**14**	**2**	**12**		
66	Выбор тематики итоговых проектов	2	0	2	29.04	
67	Анализ выбранной темы. Поиск информации.	2	0	2	06.05	
68	Проектная деятельность. Обработка информации.	2	0	2	13.05	
69	Проектная деятельность. Оформление проектов	2	0	2	15.05	
70	Проектная деятельность. Работа над проектом	2	1	1	20.05	
71	Проектная деятельность. Предзащита проектов	2	1	1	22.05	
72	Итоговая аттестация. Проектная деятельность. Защита проектов	2	0	2	27.05	
	Итого:	**144**	**37**	**107**		

Приложение 3

Группа - ЦГ3

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
	Введение	**2**	**1**	**1**		
1	Вводный инструктаж по ТБ. Входной контроль. Знакомство с предметом	2	1	1	05.09	
	Раздел 1. Изучение пакета прикладных программ для обработки информации	**24**	**6**	**18**		
2	Изучение текстовых редакторов. Изучение интерфейса	2	1	1	07.09	
3	Работа с клавиатурой в текстовом редакторе	2	0	2	11.09	
4	Работа в текстовом редакторе	2	0	2	14.09	
5	Презентации и из возможности. Правила созданий презентаций	2	1	1	18.09	
6	Работа с презентациями	2	1	1	21.09	
7	Создание презентаций определенной тематики	2	0	2	25.09	
8	Программы для работы с электронными таблицами	2	1	1	28.09	
9	Работа с электронными таблицами	2	0	2	02.10	
10	Расчеты в электронных таблицах	2	1	1	05.10	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
11	Изучение графических редакторов	2	1	1	09.10	
12	Работа в графическом редакторе	2	0	2	12.10	
13	Создание рисунков на свободную тему	2	0	2	16.10	
	Раздел 2. Безопасность общения	**24**	**8**	**16**		
14	Электронная почта, виды	2	1	1	19.10	
15	Правила защиты электронной почты	2	1	1	23.10	
16	Настройка шифрования в почтовых клиентах	2	0	2	26.10	
17	Социальная сеть. История социальных сетей. Мессенджеры	2	1	1	30.10	
18	Правила добавления друзей в социальных сетях. Правила сетевого общения	2	1	1	02.11	
19	Анализ общения обучающихся в социальных сетях	2	0	2	06.11	
20	Профиль пользователя. Анонимные социальные сети	2	1	1	09.11	
21	Сложные пароли. Правила хранения паролей	2	1	1	13.11	
22	Настройки конфиденциальности в социальных сетях и мессенджерах	2	0	2	16.11	
23	Виды аутентификации. Настройки безопасности аккаунта	2	0	2	20.11	
24	Публикация личной информации	2	1	1	23.11	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
25	Правила ведения публичных страниц	2	1	1	27.11	
	Раздел 3. Анализ мнений интернет-пользователей	**16**	**4**	**12**		
26	Изучение платформы «Крибрум». Работа с информацией в системе	2	1	1	30.11	
27	Поиск информации в интернет-пространстве	2	1	1	04.12	
28	Поиск информации в системе «Крибрум»	2	0	2	07.12	
29	Работа с информацией в системе «Крибрум»	2	1	1	11.12	
30	Работа с данными исследований. Визуализация	2	0	2	14.12	
31	Обобщение информации из разных источников	2	0	2	18.12	
32	Использование методов отработки информации	2	0	2	21.12	
33	Описание результатов исследования в системе «Крибрум»	2	1	1	25.12	
	Раздел 4. Распознавание опасного и вредного контента в интернет-пространстве	**14**	**4**	**10**		
34	Промежуточная аттестация. Виды опасного контента и его распознавание	2	1	1	28.12	
35	Повторный инструктаж по ТБ. Мошенничество, опасные виды деятельности	2	0	2	11.01	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
36	Определение каналов распространения опасного контента	2	1	1	15.01	
37	Анализ распространения информации о сборе средств, конкурсах, акциях, продажах в системе «Крибрум»	2	0	2	18.01	
38	Оказание поддельных услуг. Подозрительные объявления	2	1	1	22.01	
39	Основные признаки подозрительного контента	2	0	2	25.01	
40	Составление карты действий при столкновении подозрительным контентом	2	1	1	29.01	
	Раздел 5. Безопасность устройств и информации на них	**32**	**8**	**24**		
41	Беспроводная связь. Уязвимость Wi-Fi-соединений	2	1	1	01.02	
42	Публичные и непубличные сети	2	0	2	05.02	
43	Правила работы в публичных сетях	2	1	1	08.02	
44	Транзакции и связанные с ними риски	2	1	1	12.02	
45	Правила совершения онлайн покупок	2	1	1	15.02	
46	Обзор сайтов онлайн-продаж	2	0	2	19.02	
47	Безопасность банковских сервисов	2	0	2	22.02	
48	Определение кибербуллинга и его виды	2	1	1	26.02	
49	Причины кибербуллинга и его последствий	2	0	2	29.02	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
50	Способы избавления от кибербуллинга. Помощь жертве кибербуллинга	2	0	2	04.03	
51	Фишинг. Популярные варианты распространения фишинга	2	1	1	07.03	
52	Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах	2	0	2	11.03	
53	Виды облачных хранилищ. Сравнительный анализ	2	1	1	14.03	
54	Совместная работа с облачными сервисами	2	0	2	18.03	
55	Безопасность личной информации	2	1	1	21.03	
56	Создание резервных копий на различных устройствах	2	0	2	25.03	
	Раздел 6. Порядок действий ликвидации последствий сбоев системы	**18**	**4**	**14**		
57	Понятие сбоя системы и кибератаки и синего экрана	2	1	1	28.03	
58	Способы распространения и заражения	2	1	1	01.04	
59	Работа с восстановлением данных	2	0	2	04.04	
60	Кража персональных данных с помощью вредоносного ПО	2	1	1	08.04	
61	Способы доставки вредоносных кодов. Вредоносная рассылка	2	0	2	11.04	
62	Распространение вредоносного кода для мобильных устройств	2	0	2	15.04	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
63	Способы распознавания вредоносных программ мобильных устройств	2	0	2	18.04	
64	Способы защиты устройств от вредоносного кода	2	1	1	22.04	
65	Антивирусные программы	2	0	2	25.04	
	Проектная деятельность	**14**	**2**	**12**		
66	Выбор тематики итоговых проектов	2	0	2	29.04	
67	Анализ выбранной темы. Поиск информации.	2	0	2	02.05	
68	Проектная деятельность. Обработка информации.	2	0	2	06.05	
69	Проектная деятельность. Оформление проектов	2	0	2	13.05	
70	Проектная деятельность. Работа над проектом	2	1	1	16.05	
71	Проектная деятельность. Предзащита проектов	2	1	1	20.05	
72	Итоговая аттестация. Проектная деятельность. Защита проектов	2	0	2	23.05	
	Итого:	**144**	**37**	**107**		

Приложение 4

Лист корректировки программы

Количество часов по программе (на начало учебного года) – 144 ч.
Количество часов по программе (на конец учебного года) -

№ занятия	Раздел	Планируемое кол-во часов	Фактическое кол-во часов	Причина корректировки	Способ корректировки	Согласованно