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

Рассмотрено
на педагогическом совете
протокол № 1
от «31» августа 2022 г.

УТВЕРЖДАЮ
Директор ГАУ ДО «Центр цифрового образования «АЙТИ-куб»
Дятьковского района»
_____ Е.Н. Короткова
Приказ № 70-од от «31» августа 2022 г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ (ОБЩЕРАЗВИВАЮЩАЯ) ПРОГРАММА
«Цифровая гигиена и работа с большими данными»

возраст обучающихся: 8-17 лет, срок реализации: 1 год

Автор-составитель:
Исаева Марина Александровна,
Дудкина Нина Петровна
педагог дополнительного образования
(квалификация)

г. Дятьково – 2022 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа «Цифровая гигиена и работа с большими данными» разработана в соответствии с:

- Федеральным Законом №273-ФЗ от 29.12.2012 г. «Об образовании в Российской Федерации».
- Конвенцией ООН о правах ребёнка.
- Приказ Министерства просвещения Российской Федерации от 09.11.2018г. № 196 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам».
- Концепцией развития дополнительного образования детей в РФ,
- Концепцией духовно-нравственного развития и воспитания личности гражданина России.
- Письмом Министерства образования и науки РФ от 18.11.2015 года №09-3242 «Методические рекомендации по проектирование общеразвивающих программ».
- Санитарно-эпидемиологическими правилами и нормативами (СанПин 2.4.4.3172-14 от 04.07.2014 зарегистрированный в Минюсте России 20.08.2014 регистр №33660.

Направленность программы

Дополнительная общеобразовательная (общеразвивающая) программа «Цифровая гигиена и работа с большими данными» (далее - программа), является технической направленностью и предназначена для использования в системе дополнительного образования детей.

Новизна и отличительные особенности

Программа в целом строится на концепции подготовки к профессии кибердследователя – профессии будущего, выделенной в «Атласе новых профессий».

В ходе освоения программы, обучающиеся получат навыки исследовательской деятельности и анализа информации в интернет-пространстве, научатся обнаруживать источники информации, каналы и способы ее распространения. Также научатся распознавать опасный и вредный контент, манипулирование сознанием и внушение потенциально опасных идей в интернет-пространстве.

Программа знакомит с методическими основами и практикой анализа информации в интернет-пространстве и демонстрирует социальную значимость аналитической работы.

Отличительной особенностью программы является использование метода дифференцированного обучения, основанного на принципах преемственности. В программе изучается полный пакет прикладных программ для обработки информации. Освоение программы происходит в основном в процессе практической творческой деятельности.

Актуальность, педагогическая целесообразность

Заключается в привлечении к занятиям техническим творчеством, что способствует развитию логического мышления, творческих способностей и навыков решения задач. 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.

Также 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.

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.

Цель Программы

Формирование у обучающихся способности к анализу информации, размещенной на различных интернет – ресурсах, в интересах безопасного и рационального использования интернет- пространства. Обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз.

Задачи Программы

Обучающие:

- сформировать представление о структуре и типах информации в интернет-пространстве, больших данных и больших пользовательских данных;
- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
- ознакомить с методами и средствами поиска информации в интернет-пространстве;
- ознакомить обучающихся с основами исследовательской деятельности;
- сформировать 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»;

- сформировать способность определять социальные характеристики и индивидуальные особенности людей и обнаруживать признаки опасного поведения на основании их аккаунтов в социальных сетях.

Развивающие:

- создание условий для развития поисковой активности, исследовательского мышления;
- развитие самостоятельности и творческого подхода к решению задач;
- развитие логического, технического мышления;
- способствовать формированию умения практического применения полученных знаний;
- сформировать у обучающихся способность выявлять и критически оценивать источники и каналы распространения информации в интернет-пространстве и определять ее качество;
- сформировать у обучающихся способность успешной самопрезентации и создания позитивного имиджа в социальных сетях;
- развивать познавательные способности ребенка, память, внимание, пространственное мышление, аккуратность и изобретательность;
- создать мотивацию 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 ребёнка;
- воспитать упорство и стремление в достижении результата;
- привить информационную культуру: ответственное отношение к информации с учетом правовых и этических аспектов её распространения, избирательного отношения к полученной информации;

- формирование информационной культуры;
- воспитание ценностного отношения к своему здоровью.

Возраст и особенности обучающихся

Возраст обучающихся, участвующих в реализации данной программы - от 9 до 13 лет. В коллектив могут быть приняты все желающие, не имеющие противопоказаний по здоровью. Количество обучающихся в одной группе варьируется от 8 до 12 человек.

Сроки реализации Программы 1 год (144 часа).

Формы и режим занятий

Формы обучения и виды занятий: 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 занятия - 45 минут. После 45 минут занятий организовывается перерыв 10 минут для проветривания помещения и отдыха обучающихся.

Планируемые результаты

Предметные результаты:

- владеть основными приемами работы в прикладных программах для обработки информации;
- сформировать представление о структуре и типах информации в интернет-пространстве, больших данных и больших пользовательских данных;
- познакомить с методами и средствами поиска информации в интернет-пространстве;
- сформировать 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»;

- сформировать у обучающихся способность выявлять и критически оценивать источники и каналы распространения информации в интернет-пространстве и определять ее качество;
- сформировать способность определять социальные характеристики и индивидуальные особенности людей и обнаруживать признаки опасного поведения на основании их аккаунтов в социальных сетях;
- сформировать у обучающихся способность 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;
- обучить приемам противодействия негативным воздействиям в интернет - пространстве;

Личностные результаты:

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

Метапредметные результаты:

- умение самостоятельно планировать последовательность своих действий для достижения поставленных целей, а также грамотно распределять свое время и ресурсы для получения максимально эффективного результата;

- умение организовать учебное сотрудничество и совместную деятельность с педагогом и сверстниками;
- умение продуктивно общаться и взаимодействовать в процессе совместной деятельности, учитывать позиции других участников деятельности, эффективно разрешать конфликты;
- умение осуществлять самостоятельный поиск информации, анализировать и обобщать её;
- способность к принятию 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:

- определение начального уровня знаний, умений и навыков;
- промежуточный контроль;
- итоговый контроль.

Итоговая аттестация осуществляется в форме презентации, защиты проекта и оценивается по 100-балльной шкале, которая переводится в один из уровней освоения образовательной программы согласно таблице:

Баллы	Уровень освоения
0–40 баллов	Низкий
41–70 баллов	Средний
71–100 баллов	Высокий

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.

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.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Формы обучения и виды обучения

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

Основной вид занятий – комбинированный, сочетающий в себе элементы теории и практики. Большинство заданий курса выполняется самостоятельно с помощью персонального компьютера и необходимых программных средств.

Материально-техническое обеспечение

- одноместные парты и стулья в соответствии с требованиями СанПиН;
- ноутбуки на каждого обучающегося и преподавателя;
- веб-камера;
- многофункциональное устройство;
- мобильная напольная стойка;
- флипчарт;
- наушники с микрофоном;
- моноблочное интерактивное устройство.

Информационное обеспечение:

- операционная система (желательно Windows);
- поддерживаемые браузеры (для работы LMS): Yandex Browser, Chrome, Chrome Mobile, Firefox, Opera.

СПИСОК ЛИТЕРАТУРЫ

Нормативные документы:

1. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 N 273-ФЗ.
2. Стратегия развития воспитания в Российской Федерации на период до 2025 года. Распоряжение Правительства Российской Федерации от 29 мая 2015 г. № 996-р.
3. Письмо Министерства образования и науки РФ от 18.11.2015г. № 09-3242. «О направлении Методических рекомендаций по проектированию дополнительных общеразвивающих программ (включая разноуровневые)».
4. Распоряжение правительства РФ от 04.09. 2014 № 1726-р «Об утверждении Концепции развития дополнительного образования детей».
5. «Основы законодательств РФ об охране здоровья граждан», утвержденные Верховным советом РФ от 22.07.1993 № 5487 – (ред. от 25.11.2009).
6. Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребёнка в РФ».
7. Федеральный закон от «Об основах охраны здоровья граждан в Российской Федерации», 2011 г.
8. Приказ Министерства просвещения России от 09.11.2018 г. № 196 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам» (Приказ № 1008 отменен).

Список литературы для педагога:

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

2. Ашманов И.С., Иванов А.А. Продвижение сайта в поисковых системах. М.: Вильямс, 2007.
3. 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.
4. Волков Б.С., Волкова Н.В., Губанов А.В. Методология и методы психологического исследования: Учебное пособие. М.: Академический проект; Фонд «Мир», 2010.
5. Гаврилов К.В. Как сделать сюжет новостей и стать медиатворцом. М: Амфора. 2007.
6. Герцог Г.А. Основы научного исследования: методология, методика, практика: учебное пособие. Челябинск: Изд-во Челяб. гос. пед. ун та, 2013.
7. 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.
8. 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.
9. Ефимова Л.Л., Кочерга С.А. Информационная безопасность детей: российский и зарубежный опыт: Монография. М.: ЮНИТИ-ДАНА, 2013.
10. Жукова Т.И., Сазонов Б.В., Тищенко В.И. Подходы к созданию единой сетевой инфраструктуры научного сообщества // Методы инновационного развития. М.: Едиториал УРСС, 2007.
11. Земсков А.И., Шрайберг Я.Л. Электронные библиотеки. М.: Либерея, 2003.
12. Кабани Ш. SMM в стиле дзен. Стань гуру продвижения в социальных сетях и новых медиа! М.: Питер, 2012.

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

14.Лукина М.М. Интернет-СМИ: Теория и практика. М.: Аспект-Пресс. 2010.

15. Машкова С. Г. Интернет-журналистика: учебное пособие. Тамбов: Изд-во ТГТУ, 200

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

17. Прокудин Д.Е. Через открытую программную издательскую платформу к интеграции в мировое научное сообщество: решение проблемы оперативной публикации результатов научных исследований // Научная периодика: проблемы и решения. 2013. № 6. С. 13-18.

18.Словарь молодежного и интернет-сленга / Авт.-сост. Н.В. Белов. Минск: Харвест, 2007.

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

20. 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.

21. Солдатова Г., Рассказова М., Лебешева М., Зотова Е., Рогендорф П. Дети России онлайн. Результаты международного проекта EU Kids Online II в России. М.: Фонд Развития Интернет, 2013.

22. Солдатова Г.У., Рассказова Е.И., Зотова Е.Ю. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования. М.: Фонд Развития Интернет, 2013.

Список литературы для учащихся:

1. 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.

2. Федоров А.В. Медиаобразование: вчера и сегодня. М: МОО ВПП ЮНЕСКО «Информация для всех», 2009.
3. Чернец В., Базлова Т. Иванова Э., Крыгина Н. Влияние через социальные сети. М.: Фонд «ФОКУС-МЕДИА», 2010.
4. Шарков Ф.И. Коммуникология. Основы теории коммуникации: учебник для бакалавров рекламы и связей с общественностью (модуль «Коммуникология»). М.: Дашков и К°, 2010.
5. Ших К. Эра Facebook. М.: Манн, Иванов и Фербер, 2011.
6. Щербаков А.Ю. Интернет-аналитика. Поиск и оценка информации в web-ресурсах. Практическое пособие. М.: Книжный мир, 2012.

Интернет-ресурсы:

- Федеральный портал «Российское образование» [Электронный ресурс]. Режим доступа: http://www.edu.ru.
- Международная федерация образования [Электронный ресурс].– Режим доступа: http://www.mfo-rus.org.
- Образование: национальный проект [Электронный ресурс]. – Режим доступа: http://www.rost.ru/projects/education/education_main.shtml
- Сайт министерства образования и науки РФ [Электронный ресурс]. – Режим доступа: http://www.mon.gov.ru.
- Планета образования: проект [Электронный ресурс]. – Режим доступа: http://www.planetaedu.ru.
- Российское школьное образование [Электронный ресурс]. – Режим доступа: http://www.school.edu.ru
- Портал «Дополнительное образование детей» [Электронный ресурс]. – Режим доступа: http://vidod.edu.ru
- Платформа «Крибрум» [Электронный ресурс]. – Режим доступа: https://my.kribrum.ru/
- 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. Знакомство с предметом «Цифровая гигиена и работа с большими данными»	2	1	1	05.09.22	
	Раздел 1. Изучение пакета прикладных программ для обработки информации	**24**	**6**	**18**		
2	Изучение текстовых редакторов. Изучение интерфейса	2	1	1	07.09.22	
3	Работа с клавиатурой в текстовом редакторе	2	0	2	12.09.22	
4	Работа в текстовом редакторе	2	0	2	14.09.22	
5	Презентации и из возможности. Правила созданий презентаций	2	1	1	19.09.22	
6	Работа с презентациями	2	1	1	21.09.22	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
7	Создание презентаций определенной тематики	2	0	2	26.09.22	
8	Программы для работы с электронными таблицами	2	1	1	28.09.22	
9	Работа с электронными таблицами	2	0	2	03.10.22	
10	Расчеты в электронных таблицах	2	1	1	05.10.22	
11	Изучение графических редакторов	2	1	1	10.10.22	
12	Работа в графическом редакторе	2	0	2	12.10.22	
13	Создание рисунков на свободную тему	2	0	2	17.10.22	
	Раздел 2. Безопасность общения	**24**	**8**	**16**		
14	Электронная почта, виды	2	1	1	19.10.22	
15	Правила защиты электронной почты	2	1	1	24.10.22	
16	Настройка шифрования в почтовых клиентах	2	0	2	26.10.22	
17	Социальная сеть. История социальных сетей. Мессенджеры	2	1	1	31.10.22	
18	Правила добавления друзей в социальных сетях. Правила сетевого общения	2	1	1	02.11.22	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
19	Анализ общения обучающихся в социальных сетях	2	0	2	07.11.22	
20	Профиль пользователя. Анонимные социальные сети	2	1	1	09.11.22	
21	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей	2	1	1	14.11.22	
22	Настройки приватности и конфиденциальности в разных социальных сетях и мессенджерах	2	0	2	16.11.22	
23	Виды аутентификации. Настройки безопасности аккаунта	2	0	2	21.11.22	
24	Публикация личной информации	2	1	1	23.11.22	
25	Правила ведения публичных страниц	2	1	1	28.11.22	
	Раздел 3. Анализ мнений интернет-пользователей	**16**	**4**	**12**		
26	Изучение платформы «Крибрум». Работа с информацией в системе	2	1	1	30.11.22	
27	Поиск информации в интернет-пространстве	2	1	1	05.12.22	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
28	Поиск информации в системе «Крибрум»	2	0	2	07.12.22	
29	Работа с информацией в системе «Крибрум»	2	1	1	12.12.22	
30	Работа с данными исследований. Визуализация	2	0	2	14.12.22	
31	Обобщение информации из разных источников	2	0	2	19.12.22	
32	Использование методов отработки информации	2	0	2	21.12.22	
33	Описание результатов исследования в системе «Крибрум»	2	1	1	26.12.22	
	Раздел 4. Распознавание опасного и вредного контента в интернет-пространстве	**14**	**4**	**10**		
34	Виды опасного контента и его распознавание	2	1	1	28.12.22	
35	Мошенничество, опасные виды деятельности	2	0	2	09.01.23	
36	Повторный инструктаж по ТБ. Определение источников и каналов распространения опасного контента	2	1	1	11.01.23	
37	Анализ распространения информации о сборе средств, конкурсах, акциях, продажах в системе «Крибрум»	2	0	2	16.01.23	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
38	Оказание поддельных услуг. Подозрительные объявления	2	1	1	18.01.23	
39	Основные признаки подозрительного контента	2	0	2	23.01.23	
40	Составление карты действий при столкновении подозрительным контентом	2	1	1	25.01.23	
	Раздел 5. Безопасность устройств и информации на них	**32**	**8**	**24**		
41	Беспроводная связь. Уязвимость Wi-Fi-соединений	2	1	1	30.01.23	
42	Публичные и непубличные сети	2	0	2	01.02.23	
43	Правила работы в публичных сетях	2	1	1	06.02.23	
44	Транзакции и связанные с ними риски	2	1	1	08.02.23	
45	Правила совершения онлайн покупок	2	1	1	13.02.23	
46	Обзор сайтов онлайн-продаж	2	0	2	15.02.23	
47	Безопасность банковских сервисов	2	0	2	20.02.23	
48	Определение кибербуллинга и его виды	2	1	1	22.02.23	
49	Причины кибербуллинга и его последствий	2	0	2	27.02.23	

№	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	01.03.23	
51	Фишинг. Популярные варианты распространения фишинга	2	1	1	06.03.23	
52	Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах	2	0	2	13.03.23	
53	Виды облачных хранилищ. Сравнительный анализ	2	1	1	15.03.23	
54	Совместная работа с облачными сервисами	2	0	2	20.03.23	
55	Безопасность личной информации	2	1	1	22.03.23	
56	Создание резервных копий на различных устройствах	2	0	2	27.03.23	
	Раздел 6. Порядок действий ликвидации последствий сбоев системы	**18**	**4**	**14**		
57	Понятие сбоя системы и кибератаки и синего экрана	2	1	1	29.03.23	
58	Способы распространения и заражения	2	1	1	03.04.23	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
59	Работа с восстановлением данных	2	0	2	05.04.23	
60	Кража персональных данных с помощью вредоносного ПО	2	1	1	10.04.23	
61	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка	2	0	2	12.04.23	
62	Распространение вредоносного кода для мобильных устройств	2	0	2	17.04.23	
63	Способы распознавания вредоносных программ мобильных устройств	2	0	2	19.04.23	
64	Способы защиты устройств от вредоносного кода	2	1	1	24.04.23	
65	Антивирусные программы	2	0	2	26.04.23	
	Проектная деятельность	**14**	**2**	**12**		
66	Проектная деятельность. Выбор тематики	2	0	2	03.05.23	
67	Проектная деятельность. Анализ выбранной темы	2	0	2	10.05.23	
68	Проектная деятельность. Поиск информации по теоретическому блоку	2	0	2	15.05.23	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
69	Проектная деятельность. Разработка практической части	2	0	2	17.05.23	
70	Проектная деятельность. Работа над проектом	2	1	1	22.05.23	
71	Проектная деятельность. Предзащита проектов	2	1	1	24.05.23	
72	Проектная деятельность. Защита проектов	2	0	2	29.05.23	
	Итого:	**144**	**37**	**107**		

Приложение 2

Календарно-тематическое планирование

Группа – **ЦГ2, 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. Знакомство с предметом «Цифровая гигиена и работа с большими данными»	2	1	1	01.09.22	
	Раздел 1. Изучение пакета прикладных программ для обработки информации	**24**	**6**	**18**		
2	Изучение текстовых редакторов. Изучение интерфейса	2	1	1	06.09.22	
3	Работа с клавиатурой в текстовом редакторе	2	0	2	08.09.22	
4	Работа в текстовом редакторе	2	0	2	13.09.22	
5	Презентации и из возможности. Правила созданий презентаций	2	1	1	15.09.22	
6	Работа с презентациями	2	1	1	22.09.22	
7	Создание презентаций определенной тематики	2	0	2	22.09.22	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
8	Программы для работы с электронными таблицами	2	1	1	27.09.22	
9	Работа с электронными таблицами	2	0	2	29.09.22	
10	Расчеты в электронных таблицах	2	1	1	04.10.22	
11	Изучение графических редакторов	2	1	1	06.10.22	
12	Работа в графическом редакторе	2	0	2	11.10.22	
13	Создание рисунков на свободную тему	2	0	2	13.10.22	
	Раздел 2. Безопасность общения	**24**	**8**	**16**		
14	Электронная почта, виды	2	1	1	18.10.22	
15	Правила защиты электронной почты	2	1	1	20.10.22	
16	Настройка шифрования в почтовых клиентах	2	0	2	25.10.22	
17	Социальная сеть. История социальных сетей. Мессенджеры	2	1	1	27.10.22	
18	Правила добавления друзей в социальных сетях. Правила сетевого общения	2	1	1	01.11.22	
19	Анализ общения обучающихся в социальных сетях	2	0	2	03.11.22	
20	Профиль пользователя. Анонимные социальные сети	2	1	1	08.11.22	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
21	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей	2	1	1	10.11.22	
22	Настройки приватности и конфиденциальности в разных социальных сетях и мессенджерах	2	0	2	15.11.22	
23	Виды аутентификации. Настройки безопасности аккаунта	2	0	2	17.11.22	
24	Публикация личной информации	2	1	1	22.11.22	
25	Правила ведения публичных страниц	2	1	1	24.11.22	
	Раздел 3.Анализ мнений интернет-пользователей	**16**	**4**	**12**		
26	Изучение платформы «Крибрум». Работа с информацией в системе	2	1	1	29.11.22	
27	Поиск информации в интернет-пространстве	2	1	1	01.12.22	
28	Поиск информации в системе «Крибрум»	2	0	2	06.12.22	
29	Работа с информацией в системе «Крибрум»	2	1	1	08.12.22	
30	Работа с данными исследований. Визуализация	2	0	2	13.12.22	
31	Обобщение информации из разных источников	2	0	2	15.12.22	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
32	Использование методов отработки информации	2	0	2	20.12.22	
33	Описание результатов исследования в системе «Крибрум»	2	1	1	22.12.22	
	Раздел 4. Распознавание опасного и вредного контента в интернет-пространстве	**14**	**4**	**10**		
34	Виды опасного контента и его распознавание	2	1	1	27.12.22	
35	Мошенничество, опасные виды деятельности	2	0	2	29.12.22	
36	Повторный инструктаж по ТБ. Определение источников и каналов распространения опасного контента	2	1	1	10.01.23	
37	Анализ распространения информации о сборе средств, конкурсах, акциях, продажах в системе «Крибрум»	2	0	2	12.01.23	
38	Оказание поддельных услуг. Подозрительные объявления	2	1	1	17.01.23	
39	Основные признаки подозрительного контента	2	0	2	19.01.23	
40	Составление карты действий при столкновении подозрительным контентом	2	1	1	24.01.23	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
	Раздел 5. Безопасность устройств и информации на них	**32**	**8**	**24**		
41	Беспроводная связь. Уязвимость Wi-Fi-соединений	2	1	1	26.01.23	
42	Публичные и непубличные сети	2	0	2	31.01.23	
43	Правила работы в публичных сетях	2	1	1	02.02.23	
44	Транзакции и связанные с ними риски	2	1	1	07.02.23	
45	Правила совершения онлайн покупок	2	1	1	09.02.23	
46	Обзор сайтов онлайн-продаж	2	0	2	14.02.23	
47	Безопасность банковских сервисов	2	0	2	16.02.23	
48	Определение кибербуллинга и его виды	2	1	1	21.02.23	
49	Причины кибербуллинга и его последствий	2	0	2	28.02.23	
50	Способы избавления от кибербуллинга. Помощь жертве кибербуллинга	2	0	2	02.03.23	
51	Фишинг. Популярные варианты распространения фишинга	2	1	1	07.03.23	

№	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	09.03.23	
53	Виды облачных хранилищ. Сравнительный анализ	2	1	1	14.03.23	
54	Совместная работа с облачными сервисами	2	0	2	16.03.23	
55	Безопасность личной информации	2	1	1	21.03.23	
56	Создание резервных копий на различных устройствах	2	0	2	23.03.23	
	Раздел 6. Порядок действий ликвидации последствий сбоев системы	**18**	**4**	**14**		
57	Понятие сбоя системы и кибератаки и синего экрана	2	1	1	28.03.23	
58	Способы распространения и заражения	2	1	1	30.03.23	
59	Работа с восстановлением данных	2	0	2	04.04.23	
60	Кража персональных данных с помощью вредоносного ПО	2	1	1	06.04.23	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
61	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка	2	0	2	11.04.23	
62	Распространение вредоносного кода для мобильных устройств	2	0	2	13.04.23	
63	Способы распознавания вредоносных программ мобильных устройств	2	0	2	18.04.23	
64	Способы защиты устройств от вредоносного кода	2	1	1	20.04.23	
65	Антивирусные программы	2	0	2	25.04.23	
	Проектная деятельность	**14**	**2**	**12**		
66	Проектная деятельность. Выбор тематики	2	0	2	27.04.23	
67	Проектная деятельность. Анализ выбранной темы	2	0	2	02.05.23	
68	Проектная деятельность. Поиск информации по теоретическому блоку	2	0	2	04.05.23	
69	Проектная деятельность. Разработка практической части	2	0	2	11.05.23	
70	Проектная деятельность. Работа над проектом	2	1	1	16.05.23	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
71	Проектная деятельность. Предзащита проектов	2	1	1	18.05.23	
72	Проектная деятельность. Защита проектов	2	0	2	23.05.23	
	Итого:	**144**	**37**	**107**		

Приложение 3

Календарно-тематическое планирование

Группа – **ЦГ4**

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
	Введение	**2**	**1**	**1**		
1	Вводный инструктаж по ТБ. Знакомство с предметом «Цифровая гигиена и работа с большими данными»	2	1	1	01.09.22	
	Раздел 1. Изучение пакета прикладных программ для обработки информации	**24**	**6**	**18**		
2	Изучение текстовых редакторов. Изучение интерфейса	2	1	1	05.09.22	
3	Работа с клавиатурой в текстовом редакторе	2	0	2	08.09.22	
4	Работа в текстовом редакторе	2	0	2	12.09.22	
5	Презентации и из возможности. Правила созданий презентаций	2	1	1	15.09.22	
6	Работа с презентациями	2	1	1	19.09.22	
7	Создание презентаций определенной тематики	2	0	2	22.09.22	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
8	Программы для работы с электронными таблицами	2	1	1	26.09.22	
9	Работа с электронными таблицами	2	0	2	29.09.22	
10	Расчеты в электронных таблицах	2	1	1	03.10.22	
11	Изучение графических редакторов	2	1	1	06.10.22	
12	Работа в графическом редакторе	2	0	2	10.10.22	
13	Создание рисунков на свободную тему	2	0	2	13.10.22	
	Раздел 2. Безопасность общения	**24**	**8**	**16**		
14	Электронная почта, виды	2	1	1	17.10.22	
15	Правила защиты электронной почты	2	1	1	20.10.22	
16	Настройка шифрования в почтовых клиентах	2	0	2	24.10.22	
17	Социальная сеть. История социальных сетей. Мессенджеры	2	1	1	27.10.22	
18	Правила добавления друзей в социальных сетях. Правила сетевого общения	2	1	1	31.10.22	
19	Анализ общения обучающихся в социальных сетях	2	0	2	03.11.22	
20	Профиль пользователя. Анонимные социальные сети	2	1	1	07.11.22	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
21	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей	2	1	1	10.11.22	
22	Настройки приватности и конфиденциальности в разных социальных сетях и мессенджерах	2	0	2	14.11.22	
23	Виды аутентификации. Настройки безопасности аккаунта	2	0	2	17.11.22	
24	Публикация личной информации	2	1	1	21.11.22	
25	Правила ведения публичных страниц	2	1	1	24.11.22	
	Раздел 3.Анализ мнений интернет-пользователей	**16**	**4**	**12**		
26	Изучение платформы «Крибрум». Работа с информацией в системе	2	1	1	28.11.22	
27	Поиск информации в интернет-пространстве	2	1	1	01.12.22	
28	Поиск информации в системе «Крибрум»	2	0	2	05.12.22	
29	Работа с информацией в системе «Крибрум»	2	1	1	08.12.22	
30	Работа с данными исследований. Визуализация	2	0	2	12.12.22	
31	Обобщение информации из разных источников	2	0	2	15.12.22	
32	Использование методов отработки информации	2	0	2	19.12.22	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
33	Описание результатов исследования в системе «Крибрум»	2	1	1	22.12.22	
	Раздел 4. Распознавание опасного и вредного контента в интернет-пространстве	**14**	**4**	**10**		
34	Виды опасного контента и его распознавание	2	1	1	26.12.22	
35	Мошенничество, опасные виды деятельности	2	0	2	29.12.22	
36	Повторный инструктаж по ТБ. Определение источников и каналов распространения опасного контента	2	1	1	09.01.23	
37	Анализ распространения информации о сборе средств, конкурсах, акциях, продажах в системе «Крибрум»	2	0	2	12.01.23	
38	Оказание поддельных услуг. Подозрительные объявления	2	1	1	16.01.23	
39	Основные признаки подозрительного контента	2	0	2	19.01.23	
40	Составление карты действий при столкновении подозрительным контентом	2	1	1	23.01.23.	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
	Раздел 5. Безопасность устройств и информации на них	**32**	**8**	**24**		
41	Беспроводная связь. Уязвимость Wi-Fi-соединений	2	1	1	26.01.23	
42	Публичные и непубличные сети	2	0	2	30.01.23	
43	Правила работы в публичных сетях	2	1	1	02.02.23	
44	Транзакции и связанные с ними риски	2	1	1	06.02.23	
45	Правила совершения онлайн покупок	2	1	1	09.02.23	
46	Обзор сайтов онлайн-продаж	2	0	2	13.02.23	
47	Безопасность банковских сервисов	2	0	2	16.02.23	
48	Определение кибербуллинга и его виды	2	1	1	20.02.23	
49	Причины кибербуллинга и его последствий	2	0	2	27.02.23	
50	Способы избавления от кибербуллинга. Помощь жертве кибербуллинга	2	0	2	02.03.23	
51	Фишинг. Популярные варианты распространения фишинга	2	1	1	06.03.23	

№	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	09.03.23	
53	Виды облачных хранилищ. Сравнительный анализ	2	1	1	13.03.23	
54	Совместная работа с облачными сервисами	2	0	2	16.03.23	
55	Безопасность личной информации	2	1	1	20.03.23	
56	Создание резервных копий на различных устройствах	2	0	2	23.03.23	
	Раздел 6. Порядок действий ликвидации последствий сбоев системы	**18**	**4**	**14**		
57	Понятие сбоя системы и кибератаки и синего экрана	2	1	1	27.03.23	
58	Способы распространения и заражения	2	1	1	30.03.23	
59	Работа с восстановлением данных	2	0	2	03.04.23	
60	Кража персональных данных с помощью вредоносного ПО	2	1	1	06.04.23	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
61	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка	2	0	2	10.04.23	
62	Распространение вредоносного кода для мобильных устройств	2	0	2	13.04.23	
63	Способы распознавания вредоносных программ мобильных устройств	2	0	2	17.04.23	
64	Способы защиты устройств от вредоносного кода	2	1	1	20.04.23	
65	Антивирусные программы	2	0	2	24.04.23	
	Проектная деятельность	**14**	**2**	**12**		
66	Проектная деятельность. Выбор тематики	2	0	2	27.04.23	
67	Проектная деятельность. Анализ выбранной темы	2	0	2	04.05.23	
68	Проектная деятельность. Поиск информации по теоретическому блоку	2	0	2	11.05.23	
69	Проектная деятельность. Разработка практической части	2	0	2	15.05.23	
70	Проектная деятельность. Работа над проектом	2	1	1	18.05.23	

№	Название раздела, темы	Общее кол-во часов	В том числе		Дата	
			Теория	Практика	План	Факт
71	Проектная деятельность. Предзащита проектов	2	1	1	22.05.23	
72	Проектная деятельность. Защита проектов	2	0	2	25.05.23	
	Итого:	**144**	**37**	**107**		