СЕТЬ ЦЕНТРОВ ЦИФРОВОГО ОБРАЗОВАНИЯ ДЕТЕЙ «IT-КУБ»

IT-Cube.Миасс

КИБЕР ГИГИЕНА

и Big Data

Муниципальное автономное учреждение
дополнительного образования
«Дом детского творчества «Юность» имени академика В.П.Макеева»
(МАУ ДО «ДДТ «Юность» им. В.П. Макеева»)

Принята на заседании
Методического совета
«31» 08 2020 г.
Протокол № 1

Утверждена:
Директор МАУ ДО «ДДТ
«Юность» им. В.П. Макеева»
_____/Темур Л.В./
«__» _____ 2020 г.

АКЦЕПТОВАНА «ФОНДОМ НОВЫХ ФОРМ РАЗВИТИЯ ОБРАЗОВАНИЯ»

IT-направление «Цифровая гигиена и работа с большими данными»

Дополнительная общеобразовательная общеразвивающая программа
технической направленности

«Кибергигиена и Big Data»

Возраст обучающихся: 10-18 лет
Срок реализации программы: 1 год
144 часа

Автор-составитель:
Фомина Софья Андреевна
педагог дополнительного образования

Миасс, 2020

Пояснительная записка

Дополнительная общеобразовательная общеразвивающая программа «**Кибергигиена и Big Data**» (далее – Программа) имеет техническую направленность и составлена на основании нормативных документов федерального и регионального уровней, а также на основании нормативных актов МАУ ДО «ДДТ «Юность» им. В.П.Макеева».

Актуальность программы обоснована острой потребностью современного российского общества в грамотном и конструктивном использовании ресурсов сети Интернет и социальных медиа. На сегодняшний день высока востребованность аналитиков, обладающих навыками работы с Big Data (большим объемом данных).

Современные условия социально-экономического развития страны требуют работы с огромными объёмами пользовательских данных для статистического и прогнозирующего анализа, способного определить запросы и настроения общества. Обучение работе с большими данными даёт возможность в дальнейшем применить полученные навыки в любой научной, социально-ориентированной или коммерческой деятельности.

Педагогическая целесообразность

Социальные сети являются неотъемлемой частью жизни большинства детей и, следовательно, их использование не может оставаться бесконтрольным. Социальные медиа являются реальным онлайн-пространством, где действуют правила не только этического, но и законодательного характера, поэтому необходима организация системы дополнительного образования в области цифровой гигиены.

Программа «Кибергигиена и Big Data» направлена на раннее развитие у детей аналитического мышления, реализацию их творческих, познавательных, исследовательских и коммуникативных потребностей.

Программа научит обучающегося грамотному использованию инструментов социальных медиа, защите от противоправных действий в сети, поможет детям понять морально-этические правила межличностного взаимодействия, даст представление о последствиях девиантного поведения и дискредитации себя или других в интернет-пространстве.

Новизна Программы

Новизна программы заключается в использовании инструментов и методов, созданных за последние два года для изучения быстро меняющегося интернет-пространства. Система мониторинга и анализа социальных медиа («Крибрум») впервые используется для обучения детей школьного возраста.

Цель и задачи программы

Цель: обучить приемам и методам самостоятельного анализа и оценки информации в интернет-пространстве в контексте личной психологической безопасности.

Задачи:

Обучающие:

- формировать представление о структуре и типах информации в интернет-пространстве, больших данных и больших пользовательских данных;
- обучить основам исследовательской деятельности (принципам построения исследования, процедурой и этикой его проведения, количественным и качественным методам обработки полученных данных);
- научить применять методы и средства поиска информации в интернет-пространстве (поисковые системы, общедоступные сайты и каталоги);
- познакомить с основными приемами противодействия негативным явлениям в интернет-пространстве и научить ими пользоваться;
- сформировать навыки распознавания опасного и вредного контента, явлений манипулирования сознанием, внушения деструктивных идей и вовлечения в социально опасные группы в социальных сетях.

Развивающие:

- развивать аналитические знания, умения и навыки;
- развивать навык индивидуальной и коллективной деятельности, направленной на создание доброжелательной, конструктивной среды в социальных медиа.

Воспитательные:

- сформировать у обучающихся интерес к аналитической деятельности;
- развивать навыки социальной коммуникации в интернет-пространстве и в реальной жизни;
- формировать способность к успешной самопрезентации и формированию позитивного имиджа в социальных сетях;
- формировать культуру позитивного и конструктивного использования интернет-пространства.

Отличительная особенность

Отличительной особенностью программы является системный подход к изучению вопросов кибербезопасности и цифровой гигиены, использование системы мониторинга социальных медиа. Педагог использует традиционные настольные, развивающие игры, адаптируя их под изучаемые в рамках дисциплины темы: кибербезопасность, социальные сети. Особенностью практики в программе для обработки больших данных является изучение возможных способов манипуляции (на примере коммерческих приёмов), в процессе которого обучающийся не сталкивается с непосредственными контент-рисками и прямым негативом в сети.

Организация образовательного процесса

Программа адресована обучающимся 10-18 лет без предварительного отбора.

Количество обучающихся в группах — 12 человек.

Режим занятий: 144 часа в год (2 занятия в неделю длительностью 2 академических часа с 10-минутным перерывом).

Срок реализации программы – 1 год.

Основанием для зачисления на обучение является заявление родителей (законных представителей несовершеннолетних) обучающихся. Занятия проводятся с учетом возрастных и индивидуальных особенностей детей.

Планируемые результаты

Предметные:

- научить понимать структуру интернет-пространства;
- знать типы источников информации и разновидности контента;
- овладеть методологией исследования информации в интернет-пространстве с помощью количественных и качественных методов;
- научиться работать с поисковыми системами, общедоступными средствами поиска информации в интернет-пространстве и системой «Крибрум»;
- формировать целостное представление об объекте, ситуации или социальной группе на основе разных источников с применением системы «Крибрум» и без неё;
- научиться выявлять признаки рискованного и опасного поведения и различных угроз в интернет-пространстве (фишинг, мошенничество, вовлечение в опасные виды деятельности), уметь идентифицировать их в социальных сетях;
- сформировать понимание и принятие правил безопасного поведения в интернет-пространстве, рационального использования персональных данных, защиты от вредоносных воздействий.

Метапредметные:

- научить определять и учитывать индивидуальные особенности людей;
- научить представлять результаты своей работы окружающим, аргументировать свою позицию;
- научить свободно ориентироваться в интернет-пространстве, использовать различные типы источников для решения научно-исследовательских задач;
- научить ставить цели, планировать свою работу и следовать намеченному плану, критически оценивать достигнутые результаты.

Личностные:

- развить аналитическое, практическое и логическое мышление;
- развить самостоятельность и самоорганизацию;
- привить умение работать в команде;
- развить коммуникативные навыки;
- научить формировать и поддерживать собственный позитивный имидж в социальных сетях;
- рационально и безопасно использовать информационные сети.

Учебный план обучения

№ п/п	Тема	Общее кол-во часов	В том числе:		Формы аттестации/ контроля
			теоретических	практических	
1	Правильный поиск информации. Вводное занятие. Знакомство с предметом.	18	6	12	Защита презентации.
2	Социальные сети и социальные медиа.	14	3	11	Защита презентации.
3	Порядок действий ликвидации последствий сбоев системы, кибератак. Возможные пути решения проблемы.	16	6	10	Интерактивный тест.
4	Анализ социальных групп на основе данных интернет-пространства.	10	2	8	Защита презентации.
5	Безопасное и рациональное использование личных и персональных данных в	20	7	13	Защита проекта (открытый урок)

	социальных сетях.				
6	Распознавание опасного и вредного контента в интернет-пространстве	18	2	16	Интерактивный тест-соревнование Защита проекта. Оценочный лист.
7	Анализ информационных сообщений в интернете	14	3	11	Защита презентации.
8	Конфликтные ситуации в социальных медиа.	12	2	10	Защита презентации.
9	Деструктивное воздействие в социальных медиа.	8	2	6	Защита презентации.
10	Безопасное поведение в сети. Проект «Научу своих близких кибергигиене».	14	3	11	Защита презентации. Защита проекта. (открытый урок). Оценочный лист.
	Итого:	144	36	108	

Содержание учебного плана 1 года обучения

1. *Вводный урок. Знакомство с предметом.*

Теория: Знакомство с предметом «Кибергигиена». Правила техники безопасности и противопожарной защиты.

Практика: Инструктаж по технике безопасности и противопожарной защите. Входной контроль. Работа с итоговой презентацией на тему раздела.

2. *Правильный поиск информации.*

Теория: Информационная структура интернета, поиск и правила поиска.

Практика: Поисковые системы, принципы оценки информации, формирование правил поиска. Работа с итоговой презентацией на тему раздела.

3. *Социальные сети и социальные медиа.*

Теория: Эволюция интернета, направления социальных медиа, элементы контента социальных сетей.

Практика: Знакомство и работа с платформой «Крибрум». Работа с итоговой презентацией на тему раздела.

4. *Порядок действий ликвидации последствий сбоев системы, кибератак. Возможные пути решения проблемы.*

Теория: Понятие сбоя системы и синего экрана. Причины. Способы восстановления системы.

Практика: Изучение фейковых сообщений, хакерской деятельности и вредоносного программного обеспечения в сети Интернет и с помощью системы «Крибрум». Прохождение интерактивного теста на тему раздела.

5. *Анализ социальных групп на основе данных интернет-пространства.*

Теория: Понятие социальная группа, сообщество, субкультура, фэндом. Правила сетевого общения.

Практика: Анализ с помощью системы «Крибрум» активности участников группы сообщества, связей, поведенческих особенностей, предпочтений и интересов сообщества. Работа с итоговой презентацией на тему раздела.

6. *Безопасное и рациональное использование личных и персональных данных в социальных сетях.*

Теория: Проблемы утечки данных, приватность, безопасные пароли.

Практика: Анализ сообщений с использованием системы «Крибрум». Работа над проектом, в соответствии с темой раздела. Участие в открытом уроке.

7. *Распознавание опасного и вредного контента в интернет-пространстве.*

Теория: Проблема контентных рисков, фишинга и негатива.

Практика: Исследования упоминаний фишинговых сайтов с помощью системы «Крибрум». Участие в интерактивном тесте-соревновании.

8. *Контрольное занятие.*

Теория: Подведение итогов пройденного материала.

Практика: Защита проекта по выбору обучающихся:

- создание тематической группы в социальной сети
- открытый мастер-класс по кибербезопасности
- создание собственной настольной игры или теста по кибербезопасности.

9. *Анализ информационных сообщений в интернете.*

Теория: Виды информационных сообщений, фейкньюс, фейки, реклама.

Практика: Работа в поисковых системах. Работа с итоговой презентацией на тему раздела.

10. *Конфликтные ситуации в социальных медиа.*

Теория: Конфликт. Признаки и условия возникновения конфликта.

Практика: Разбор конфликтных видеороликов из социальных медиа. Работа с итоговой презентацией на тему раздела.

11. *Деструктивное воздействие в социальных медиа.*

Теория: Технология геймификации. Воронка вовлечения.

Практика: Изучение деструктивного движения. Работа с итоговой презентацией на тему раздела.

12. *Безопасное поведение в сети.*

Теория: Персональная информация. Правила обращения.

Практика: Изучение аккаунта на признаки уязвимости опасностям. Работа с итоговой презентацией на тему раздела.

13. *Проект «Научу своих близких кибергигиене»*

Теория: Подведение итогов года.

Практика: Итоговое занятие - разработка, создание и защита проекта «Научу своих близких кибергигиене».

Планируемые результаты обучения

По окончанию 1 года обучения, обучающиеся будут

Знать:

- структуру интернет-пространства;
- типы источников информации и разновидности контента;
- методологию исследования информации в интернет-пространстве с помощью количественных и качественных методов;
- признаки рискованного и опасного поведения и различных угроз в интернет-пространстве (фишинг, мошенничество, вовлечение в опасные виды деятельности);

- средства защиты от вредоносных воздействий.

Уметь:

- осуществлять исследование информации в интернет-пространстве при помощи общедоступных средств поиска и системы мониторинга и анализа социальных медиа «Крибрум»;
- обрабатывать и представлять перед аудиторией результаты своего исследования;
- избегать и устранять последствия кибератак, сбоев системы;
- определять опасный контент и опасных пользователей в сети Интернет;
- грамотно реагировать на попытки манипуляции или психологического давления в сети.

Методическое обеспечение

Педагогические технологии:

Личностно-ориентированная технология;
Технология игровой деятельности;
Технология группового обучения;
Технология проблемного обучения;
Технология проектной деятельности.

Программой предусмотрены фронтальная, групповая и индивидуальная формы обучения.

Формы организации урока:

- *интерактивная лекция;*
- *практическая работа;*
- *самостоятельная работа (индивидуально или в малых группах);*
- *семинар;*
- *учебная игра;*
- *защита проекта;*
- *дебаты;*
- *контрольное занятие;*
- *конференция.*

Методы и приемы обучения:

- *проблемное изложение;*
- *информационный рассказ;*
- *иллюстрация;*
- *демонстрация наглядного материала;*
- *изучение источников;*
- *беседа;*
- *дискуссия;*
- *мозговой штурм;*
- *игровые ситуации;*
- *упражнение;*
- *частично-поисковый (эвристический) метод;*

– *метод кейсов;*
– *исследовательский метод;*
– *устный опрос;*
– *публичное выступление;*
– *наставничество.*

Педагогический контроль

Вид контроля	*Формы*	*Срок контроля*
Входной	- оценочный лист	Сентябрь
Текущий	- презентация групповых исследований,	В течение учебного года
Промежуточный	- интерактивная викторина, - презентация исследований, - защита проекта	По завершении пройденного раздела
Итоговый	- защита проекта, - оценочный лист	Май

Входной контроль 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).

Результаты входного контроля фиксируются в бланке входного контроля (Приложение 2) с использованием следующей шкалы:

Оценка параметров	Уровень по сумме баллов
Начальный уровень – 0 баллов Средний уровень – 1 балл	Высокий уровень: 9–10 баллов Средний уровень: 4–8 баллов

Высокий уровень – 2 балла	Минимальный уровень: 0–3 балла

Текущий контроль осуществляется на занятиях в течение всего учебного года для отслеживания уровня освоения учебного материала по разделам Программы.

Формы:

- соревнование-игра заключается в использовании естественной для детей склонности к соперничеству: на каждом занятии отмечаются не только лидеры, но и дети, достигшие локального успеха (сравнение с самим собой);
- фото- и видеосъемка удачных моментов («самая хорошая презентация», «кто отлично помогает младшим» и т. п.);
- выполнение контрольных заданий для оценки практических навыков, внимательности, креативности.

Промежуточный контроль осуществляется в конце каждой освоенной темы (кейса) и проводится в форме:

- презентации работ, на которой обучающиеся демонстрируют уровень овладения теоретическим и практическим программным материалом;
- интерактивного тестирования, где обучающиеся соревнуясь между собой отвечают на вопросы по теме (учитывается правильность и скорость ответов);
- открытого урока, который проводят сами обучающиеся, выступающие в роли педагогов для приглашённых родственников.

Итоговый контроль в форме защиты проекта проводится по окончании обучения, результаты отображаются в оценочном листе (Приложение 3).

Материально-техническое обеспечение

- Оборудование аудитории:

стол компьютерный для обучающихся (размер – достаточный для размещения за одним столом двоих обучающихся) – 12 шт.;

стол компьютерный для преподавателя – 1 шт. ;

стул офисный на колесиках с регулируемой высотой сиденья и наклоном спинки – 13 шт.;

магнитно-маркерная доска – 1 шт.

- Компьютерное оборудование:

стационарные персональные компьютеры (системный блок, монитор, клавиатура USB, мышь USB) с доступом в интернет – 13 шт.;

наушники проводные – 13 шт.;

акустическая система – 1 шт.;

вебкамера – 1 шт.

- Презентационное оборудование:

проектор с проекционным экраном – 1 шт.;

пульт для дистанционного переключения слайдов – 1 шт.

- Программное обеспечение:

система «Крибрум» с массивами данных для кейсов;
пакет «Microsoft Office»;
браузер «Google Chrome», «Mozilla Firefox» или «Яндекс Браузер».
Сервис для построения лент времени с возможностью совместной работы на усмотрение преподавателя (http://www.timetoast.com и т.п.).
Сервис для создания интеллект-карт с возможностью совместной работы (https://realtimeboard.com/ru/, https://www.mindmeister.com/ru и т.п.).

Расходные материалы:

Бумага А4.
Маркеры для магнитно-маркерной доски.
Губка для магнитно-маркерной доски.

Методические материалы:

Учебно-методический комплект для преподавателя (программа, описание кейсов, опорные теоретические материалы для наставников, список ресурсов).
Руководство пользователя системы «Крибрум».

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. Баскаков А.Я., Туленков Н.В. Методология научного исследования: Учеб. пособие. К.: МАУП, 2004.
4. Бек У. Общество риска. На пути к другому модерну. М.: Прогресс Традиция, 2000.
5. Бережнова Е.В., Краевский В.В. Основы исследовательской деятельности студентов: учеб. пособие для студ. сред. учеб. заведений. М.: Издат. центр «Академия», 2007.
6. Бехтерев С.В. Майнд-менеджмент. Решение бизнес-задач с помощью интеллект-карт. М.: Альпина Паблишер, 2012.
7. 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.
8. Бодалев А.А., Столин В.В. Общая психодиагностика. СПб.: Речь, 2000.
9. Брайант Д., Томпсон С. Основы воздействия СМИ. М: Издательский дом «Вильяме», 2004.
10. Волков Б.С., Волкова Н.В., Губанов А.В. Методология и методы психологического исследования: Учебное пособие. М.: Академический проект; Фонд «Мир», 2010.
11. Гаврилов К.В. Как сделать сюжет новостей и стать медиатворцом. М: Амфора. 2007.
12. Герцог Г.А. Основы научного исследования: методология, методика, практика: учебное пособие. Челябинск: Изд-во Челяб. гос. пед. ун та, 2013.
13. 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.
14. 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.
15. Елисеев О.П. Практикум по психологии личности. СПб.: Питер, 2001.
16. Ефимова Л.Л., Кочерга С.А. Информационная безопасность детей: российский и зарубежный опыт: Монография. М.: ЮНИТИ-ДАНА, 2013.
17. Жукова Т.И., Сазонов Б.В., Тищенко В.И. Подходы к созданию единой сетевой инфраструктуры научного сообщества // Методы инновационного развития. М.: Едиториал УРСС, 2007.
18. Земсков А.И., Шрайберг Я.Л. Электронные библиотеки. М.: Либерея, 2003.
19. Кабани Ш. SMM в стиле дзен. Стань гуру продвижения в социальных сетях и новых медиа! М.: Питер, 2012.

20. Кравченко А.И. Методология и методы социологических исследований. Учебник. М.: Юрайт, 2015.
21. Крупник А.Б. Поиск в Интернете: самоучитель. СПБ.: Питер, 2004.
22. Лукина М.М. Интернет-СМИ: Теория и практика. М.: Аспект-Пресс. 2010.
23. Машкова С. Г. Интернет-журналистика: учебное пособие. Тамбов: Изд-во ТГТУ, 2006.
24. Муромцев Д.И., Леманн Й., Семерханов И.А., Навроцкий М.А., Ермилов И.С. Исследование актуальных способов публикации открытых научных данных в сети // Научно-технический вестник информационных технологий, механики и оптики. 2015. Т. 15. № 6. С. 1081-1087.
25. Попов А. Блоги. Новая сфера влияния. М.: Манн, Иванов и Фербер, 2008. 22
26. 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.
27. Прохоров А. Интернет: как это работает. СПб.: БХВ - Санкт-Петербург, 2004.
28. Рубинштейн С. Л. Основы общей психологии. СПб.: Издательство «Питер», 2000. 29. Словарь молодежного и интернет-сленга / Авт.-сост. Н.В. Белов. Минск: Харвест, 2007.
30. Слугина Н. Активные пользователи социальных сетей Интернета. СПб.: Питер, 2013.
31. 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.
32. 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.
33. Солдатова Г.У., Рассказова Е.И., Зотова Е.Ю. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования. М.: Фонд Развития Интернет, 2013.
34. 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.
35. Сорокина Е., Федотченко В., Чабаненко К. В социальных сетях. Twitter: 140 символов самовыражения. М.: Питер, 2011.
36. Федоров А.В. Медиаобразование: вчера и сегодня. М: МОО ВПП ЮНЕСКО «Информация для всех», 2009.
37. Чернец В., Базлова Т. Иванова Э., Крыгина Н. Влияние через социальные сети. М.: Фонд «ФОКУС-МЕДИА», 2010.
38. Шарков Ф.И. Коммуникология. Основы теории коммуникации: учебник для бакалавров рекламы и связей с общественностью (модуль «Коммуникология»). М.: Дашков и К°, 2010.

39. Ших К. Эра Facebook. М.: Манн, Иванов и Фербер, 2011.
40. Щербаков А.Ю. Интернет-аналитика. Поиск и оценка информации в web-ресурсах. Практическое пособие. М.: Книжный мир, 2012.

Для обучающихся и родителей:

1. Новые медиа. Социальная теория и методология исследований. Словарь-справочник. СПб.: Алетейя, 2016.
2. Эрик Куалман. Безопасная Сеть. Правила сохранения репутации в эпоху социальных медиа и тотальной публичности. Альпина Паблишер, 2017.
3. Су Кеннет, Анналин Ын. Теоретический минимум по Big Data. Всё что нужно знать о больших данных. Спб.: 2019.

Приложение 1
к дополнительной общеобразовательной
общеразвивающей программе

Календарный учебный график на 2019-2020 учебный год (1, 2, 3 группы, 1 год обучения) по программе «Кибергигиена и Big Data».
Педагог: Ивахненко А.А.

Место проведения занятий: МАУ ДО «ДДТ «Юность» им. В.П. Макеева», г. Миасс, пр. Макеева, 39

№ занятия	Число, месяц	Вид учебной деятельности	Кол-во часов	Тема занятия	Форма контроля
1	Сентябрь	Практическая работа. Учебная игра.	2	Вводное занятие: «Кибергигиена» - это? Знакомство друг с другом. Коммуникативные игры. Правила техники безопасности и противопожарной защиты.	
2	Сентябрь	Самостоятельная работа. Дебаты.	2	«Что мы знаем?», «Что нам интересно?»	Входной контроль оценочный лист
3	Сентябрь	Интерактивная лекция. Самостоятельная работа.	2	Основы эффективной презентации.	
4	Сентябрь	Интерактивная лекция. Самостоятельная работа.	2	Основы эффективной самопрезентации.	
5	**Сентябрь**	**Контрольное занятие.**	**2**	**Разработка и защита презентации на выбранную тему.**	**Защита презентации.**
6	Сентябрь	Интерактивная лекция. Самостоятельная работа.	2	Знакомство с поисковыми системами. Работа в команде.	
7	Сентябрь	Интерактивная лекция. Самостоятельная работа.	2	Эффективный поиск в интернете.	
8	Сентябрь	Интерактивная лекция. Самостоятельная работа. Практическая работа.	2	Правила поиска информации.	
9	**Октябрь**	**Контрольное занятие.**	**2**	**Подготовка и защита презентации**	**Защита презентации.**

				«Эффективный поиск в интернете»	
10	Октябрь	Интерактивная лекция. Дебаты.	2	Социальные сети и социальные медиа. Проблема лайков.	
11	Октябрь	Интерактивная лекция.	2	Элементы и виды контента социальных сетей.	
12	Октябрь	Интерактивная лекция. Самостоятельная работа.	2	Программы и методы исследования социальных сетей.	
13	Октябрь	Практическая работа. Самостоятельная работа.	2	Анализ социальных сетей на предмет упоминаний фильма, сообщений и авторов с помощью системы «Крибрум».	
14	Октябрь	Семинар. Самостоятельная работа.	2	Альтернативный способ анализа: сбор информации на тематических сайтах (kinopoisk).	
15	Октябрь	Практическая работа.	2	Разработка и подготовка презентации результатов команды по анализу сообщений о фильме в системе Крибрум.	
16	**Октябрь**	**Защита проекта.**	**2**	**Демонстрация и защита презентации по анализу сообщений.**	**Защита презентации**
17	Октябрь	Интерактивная лекция. Самостоятельная работа.	2	Изучение понятия сбоя системы и синего экрана. Способы восстановления системы.	
18	Ноябрь	Интерактивная лекция. Самостоятельная работа.	2	Изучение фейковых сообщений и вредоносного ПО в сети.	
19	Ноябрь	Интерактивная лекция. Самостоятельная работа.	2	Рассмотрение наиболее крупных взломов системы и кибератак.	
20	Ноябрь	Интерактивная лекция. Самостоятельная работа.	2	Обсуждение проблемы хакерства.	
21	Ноябрь	Интерактивная лекция. Практическая работа.	2	Проблема краж персональных данных с помощью вредоносного ПО. Способы защиты от них.	
22	Ноябрь	Практическая работа.	2	Проблема краж с помощью банковских карт. Способы защиты от них.	

23	**Ноябрь**	**Контрольное занятие.**	**2**	**Презентация результатов исследования в группах или индивидуально. Проведение интерактивной викторины.**	**Интерактивный тест.**
24	**Ноябрь**	**Учебная игра.**	**2**	**Настольная игра по теме кибербезопасности.**	
25	Ноябрь	Семинар.	2	Изучение понятия социальная группа, сообщество, субкультура, фэндом. Их особенностей.	
26	Декабрь	Практическая работа.	2	Изучение структуры сообщества, авторов сообщений в социальной сети «ВКонтакте».	
27	Декабрь	Семинар.	2	Правила функционирования сетевых сообществ. Правила сетевого общения.	
28	Декабрь	Практическая работа.	2	Анализ активности участников группы сообщества.	
29	**Декабрь**	**Конференция.**	**2**	**Презентация результатов исследования индивидуально или в группах. Обсуждение результатов.**	**Защита презентации**
30	Декабрь	Интерактивная лекция.	2	Защищенность данных в сети. Проблемы утечки данных.	
31	Декабрь	Семинар.	2	Разработка рекомендаций по созданию безопасных паролей и их хранению.	
32	Декабрь	Семинар.	2	Персональные данные (ПД). Законодательство о защите ПД.	
33	Декабрь	Интерактивная лекция. Практическая работа.	2	Социальные сети: пользовательские соглашения, права и обязанности. Что в них и почему их надо читать?	
34	Январь	Интерактивная лекция. Практическая работа.	2	Политика социальных сетей в области конфиденциальности пользовательских данных. Дискуссия на тему «Мой аккаунт – моя крепость?»	
35	Январь	Практическая работа.	2	Настройки приватности, самопрезентация пользователя в социальных сетях.	
36	Январь	Интерактивная лекция. Практическая работа.	2	Риски нерационального и небезопасного использования личных и персональных данных в соцсетях.	

37	Январь	Практическая работа.	2	Проблемы рискованного поведения, манипулирования и вовлечения в опасное поведение в соцсетях.	
38	Январь	Практическая работа.	2	Подготовка проекта открытого занятия по кибербезопасности.	
39	**Январь**	**Защита проекта.**	**2**	**Проведение открытого урока для родителей и родственников обучающихся, где в роли лекторов выступают сами дети.**	**Защита проекта (открытый урок)**
40	Февраль	Интерактивная лекция. Самостоятельная работа.	2	Проблема контентных рисков и меры противодействия им.	
41	Февраль	Самостоятельная работа.	2	Механизмы защиты социальных сетей от негативного контента.	
42	Февраль	Интерактивная лекция. Самостоятельная работа.	2	Проблема фишинга в сети. Изучение вопроса с помощью системы «Крибрум».	
43	Февраль	Интерактивная лекция. Самостоятельная работа.	2	Риски потребительского поведения. Правила социальных сетей по размещению рекламы.	
44	Февраль	Интерактивная лекция. Самостоятельная работа.	2	Торговля в интернете. Изучение приёмов воздействия коммерческих организаций с помощью системы «Крибрум».	
45	Февраль	Практическая работа.	2	Проблема оказания поддельных услуг и распространения подозрительных объявлений об удаленной работе в социальных сетях.	
46	Февраль	Практическая работа.	2	Интернет: позитивное использование	
47	Февраль	Контрольное занятие.	2	Проведение интерактивной соревновательной викторины среди обучающихся.	
48	**Март**	**Защита проекта.**	**2**	**Защита группового проекта на тему, выбранную учащимися.**	**Защита проекта. Оценочный лист**
49	Март	Интерактивная лекция. Самостоятельная работа.	2	Виды информационных сообщений в интернете.	
50	Март	Интерактивная лекция. Самостоятельная работа.	2	Фейкньюс, фейки, реклама.	

51	Март	Практическая работа.	2	Фактчекинг.	
52	Март	Интерактивная лекция. Самостоятельная работа.	2	Источники и каналы распространения информации.	
53	Март	Практическая работа.	2	Рекламные сообщения в интернете	
54	Март	Практическая работа.	2	Вирусные сообщения, флешмобы, челленджи.	
55	**Март**	**Защита проекта.**	**2**	**Презентация сценария видеоролика по выбранной теме.**	**Защита презентации.**
56	Апрель	Интерактивная лекция. Самостоятельная работа.	2	Конфликтные ситуации в социальных медиа	
57	Апрель	Семинар.	2	Противостояние агрессии в сети	
58	Апрель	Семинар.	2	Правила конструктивного общения в сети	
59	Апрель	Практическая работа.	2	Как вести полемику	
60	Апрель	Интерактивная лекция. Самостоятельная работа	2	Разработка программы предотвращения кибербуллинга	
61	**Апрель**	**Защита проекта.**	**2**	**Защита программы предотвращения кибербуллинга.**	**Защита презентации.**
62	Апрель	Интерактивная лекция. Самостоятельная работа.	2	Технология геймификации.	
63	Апрель	Интерактивная лекция. Самостоятельная работа.	2	Деструктивное воздействие в социальных медиа.	
64	Апрель	Семинар.	2	Деструктивные группы и выходы из них.	
65	**Май**	**Контрольное занятие.**	**2**	**Презентация результатов по анализу деструктивного движения.**	**Защита презентации.**
66	Май	Интерактивная лекция. Самостоятельная работа.	2	Использование персональной информации пользователя злоумышленниками.	
67	Май	Семинар.	2	Правила безопасного обращения с персональными данными в социальных медиа.	
68	Май	Семинар.	2	Правила взаимодействия со злоумышленниками.	
69	Май	Дебаты.	2	Урон репутации и правонарушения в сети.	
70	**Май**	**Контрольное занятие.**	**2**	**Презентация итогов анализа «Обнаружь злоумышленника».**	**Защита презентации.**
71	Май	Практическая работа.	2	Разработка проекта «Научу своих близких кибергигиене».	
72	**Май**	**Защита проекта.**	**2**	**Защита проекта «Научу своих близких кибергигиене».**	**Защита проекта (открытый урок)**

					Оценочный лист.

Приложение 2
к дополнительной общеобразовательной
общеразвивающей программе

Бланк входного контроля

Направление «Кибергигиена», группа № _____, год обучения _____.
Ф.И.О. учащегося
_____
«___» _____ 201_ г.

№	Вопросы / задания	Оценки		
		баллы	сумма по разделу	Примечания
1	Техника безопасности	0–2		
2	Мотивированность	0–2		
3	Зрелость	0–2		
4	Умелость	0–2		
5	Владение терминологией	0–2		
	Итого	1–10		

Высокий уровень: 8–10 баллов.
Средний уровень: 4–7 баллов.
Допустимый (низкий) уровень обучения: 0–3 балла.

Вывод:
_____
_____

Требуют особого педагогического внимания:
- учащиеся с результатом менее 4 баллов;
- учащиеся с результатом более 8 баллов.

Приложение 3
к дополнительной общеобразовательной
общеразвивающей программе

Бланк итогового контроля

Направление «Кибергигиена», группа № _____, год обучения _____.
Ф.И.О. учащегося
_____
«___» _____ 201_ г.

№	Вопросы / задания	Оценки		
		Баллы	Сумма по разделу	Предыдущий балл
1	Техника безопасности	1–3		
2	Мотивированность	1–3		
3	Зрелость	1–3		
4	Умелость	1–3		
5	Владение терминологией	1–3		
	Итого	5–15		

Успешно пройденное обучение: 10–15 баллов.

Вывод:
_____
_____

Приложение 4
к дополнительной общеобразовательной
общеразвивающей программе

Дополнительная общеобразовательная общеразвивающая программа «Кибергигиена и Big Data» имеет техническую направленность и составлена на основании:

1. Закона РФ «Об образовании в Российской Федерации» (№273-ФЗ от 29.12.2012);
2. Концепции развития дополнительного образования детей (утвержденная распоряжением Правительства РФ от 04.09.2014 г. №1726-р);
3. Приказа Министерства просвещения РФ от 09.11.2018 № 196 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
4. Постановления Главного государственного санитарного врача РФ от 4.07.2014 г. № 41 «Об утверждении СанПиН 2.4.4.3172-14 «Санитарно-эпидемиологические требования к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей»;
5. Методических рекомендаций по проектированию дополнительных общеразвивающих программ, разработанных Министерством образования и науки России совместно с ГАОУ ВО «Московский государственный педагогический университет», ФГАУ «Федеральный институт развития образования» и АНО дополнительного профессионального образования «Открытое образование» (письмо Министерства образования и науки России от 18.11.2015 № 09-3242 «О направлении информации»)
6. Стратегии развития воспитания в Российской Федерации на период до 2025 года (Распоряжение Правительства РФ от 25 мая 2015г. № 996-р);
7. Закона Челябинской области от 29.08.2013 года № 515-ЗО «Об образовании в Челябинской области»;
8. Устава Муниципального автономного учреждения дополнительного образования «Дом детского творчества «Юность» имени академика В.П. Макеева»;
9. Локальных актов Учреждения:

· Положение об организации образовательного процесса;

· Положение о дополнительной общеобразовательной общеразвивающей программе;

· Положение о формах, периодичности и порядке организации и осуществления текущего контроля успеваемости, промежуточной и итоговой аттестации учащихся.