ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«ЦЕНТР ДЛЯ ОДАРЕННЫХ ДЕТЕЙ «ПОИСК»

РЕКОМЕНДОВАНА:
педагогическим советом
Протокол №6 от «2 »апреля 2024г.

УТВЕРЖДАЮ:
Заведующая филиалом
_____ Т.В. Ларина

Дополнительная общеобразовательная общеразвивающая
программа технической направленности

«ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ»

Возраст обучающихся: 14-17 лет

Объем программы: 108 часов

Срок освоения: 1 год

Форма обучения: очная

Авторы программы: Жалыбина Юлия Витальевна, заведующий ЦЦО «IT-куб»

Михайловск, 2024

ОГЛАВЛЕНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа «Персональная кибербезопасность» разработана в соответствии с требованиями нормативных документов:

Федерального закона РФ от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации».

Концепции развития дополнительного образования детей, утвержденной распоряжением Правительства РФ от 4 сентября 2014 г. № 1726-р.

Приказа Минпросвещения РФ от 09.11.2018 г. N 196 «Об утверждении

Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам».

Постановления Главного государственного санитарного врача РФ от 28.09.2020 г. № 28 СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи».

Методических рекомендаций по проектированию дополнительных общеразвивающих программ (письмо Минобрнауки РФ от 18.11.2015 г. N 09-3242).

Методических рекомендаций по созданию и функционированию центров цифрового образования «IT-куб» (утв. распоряжением Министерства просвещения Российской Федерации от 12.01.2021 № Р-5). Паспорт национального проекта «Образование» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24.12.2018 № 16).

Государственной программы Российской Федерации «Развитие образования» (утв. постановлением Правительства РФ от 26.12.2017 № 1642 (ред. от 15.03.2021) «Об утверждении государственной программы Российской Федерации “Развитие образования”»).

Стратегии развития воспитания в Российской Федерации на период до 2025 года (утв. распоряжением Правительства РФ от 29.05.2015 № 996-р «Об

утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года»).

1. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ПРОГРАММЫ

1.1. Направленность программы

Дополнительная общеобразовательная общеразвивающая программа «Персональная кибербезопасность» имеет техническую направленность.

1.2. Адресат программы

Программа адресована обучающимся от 14 до 17 лет.

Программа предназначена для одаренных школьников 7-10 классов, проявляющих повышенный интерес к информатике, математике, анализу данных.

Возрастная категория обучающихся – разновозрастная.

Необходимы базовые знания по следующим школьным предметам: информатика, математика.

Наличие определенной физической и практической подготовки для изучения учебной программы не требуется.

1.3. Актуальность программы

Программа знакомит обучающихся с основами информационной безопасности, с методическими основами и практикой анализа информации в интернет-пространстве и демонстрирует социальную значимость аналитической работы. Программа рассчитана на школьников, которые уверенно владеют основами с персональным компьютером и сетью Интернет.

1.4. Новизна программы

Новизна дополнительной общеобразовательной программы «Персональная кибербезопасность» заключена в достижении метапредметных результатов и

предметных умений дисциплины «Информатика» по формированию навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в сети интернет, умений соблюдать нормы информационной этики и права.

Уровень освоения программы – базовый.

1.5 Объем и срок освоения программы

Объем программы – 108 часов.

Срок реализации программы – 1 год.

1.6 Цели и задачи программы

Цель - создание условий формирования у обучающихся цифровой культуры личности с необходимыми навыками и присущими ценностями, взглядами, ориентациями, установками, мотивами деятельности и поведения для обеспечения безопасной и развивающей жизнедеятельности обучающегося в сети Интернет.

Задачи программы

1. Обучающие:

На основе имеющиеся у обучающихся знаний и умений углубить и систематизировать познания в области персональной кибербезопасности:

– сформировать систему общих понятий в сфере информационной безопасности;

– обучить элементам системного мышления;

– отработать навыки и умения безопасного поведения в сети интернет и полезного использования информационных технологий.

2. Развивающие:

Обучающиеся в процессе изучения образовательной программы получат возможность:

– развивать навыки сетевого общения и коммуникации в сети Интернет, поиска и работы с информацией, обеспечения безопасности цифровых устройств и аккаунтов и осуществления сетевых покупок;

– развивать умение сравнивать, выявлять сходство и различие, анализировать и делать выводы;

– совершенствовать стремление школьников к познанию, расширению кругозора, информированности в рамках предметной области;

– способствовать развитию коммуникативных навыков, психологической совместимости и адаптации в учебной группе.

3. Воспитательные:

В процессе изучения образовательной программы обучающиеся смогут:

– воспитывать культуру общения и поведения в сетевом пространстве;

– содействовать выработке целесообразных ценностных ориентаций, потребностей и мотивов поведения школьника в сфере компьютерного обеспечения.

1.7. Планируемые результаты освоения программы

1. Предметные результаты:

– сформированы основные понятия информационной безопасности, частности кибербезопасности.

– сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет.

– сформированы умения соблюдать нормы информационной этики.

– сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

2. Метапредметные результаты:

– развивается познавательная и творческая активность в безопасном

использовании информационных и коммуникационных технологий.

3. Личностные результаты:

– вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;

– стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

2. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

2.1 Язык реализации программы

Реализация дополнительной общеобразовательной общеразвивающей программы «Персональная кибербезопасность» осуществляется на государственном языке Российской Федерации.

2.2. Форма обучения:

– очная.

2.3. Особенности реализации программы

Программа реализуется по модульному принципу.

2.4. Условия набора и формирования групп

Условия набора обучающихся.

На обучение зачисляются обучающиеся 7-10 классов общеобразовательных организаций Ставропольского края.

Зачисление на обучение по программе осуществляется по результатам конкурсного отбора в соответствии с Правилами приема обучающихся в региональный центр «Сириус 26» на 2023 – 2024 учебный год.

Условия конкурсного отбора гарантируют соблюдение прав обучающихся в области дополнительного образования и обеспечивают зачисление наиболее способных и подготовленных обучающихся к освоению программы.

Условия формирования групп: разновозрастная.

2.5. Формы организации и проведение занятий

Формы организации занятий:

– аудиторные (под непосредственным руководством преподавателя).

Формы проведения занятий:

- теоретические;
- практические;
- лабораторные;
- контрольные.

Формы организации деятельности обучающихся:

Интерактивные проблемные лекции - предполагает наиболее полное вовлечение всех участников лекционного занятия в процесс изучаемого материала, демонстрация слайд-презентации или фрагментов учебных фильмов.

Мозговой штурм - предполагает генерацию идей, которую применяют для выявления проблем или поиска решений

Практикум – предполагает выполнение практических заданий.

Режим занятий.

Очная форма обучения: 7-10 классы – 3 урока 1 раз в неделю. Программа реализуется в г. Михайловске.

УЧЕБНЫЙ ПЛАН

Наименование модуля, учебного курса	Количество часов			
	Теория	**Практика**	**Всего**	**Форма контроля/ аттестации**
Модуль 1. Общие сведения об информационной безопасности.	29	19	48	Контрольный тест
Модуль 2. Основы персональной кибербезопасности.	31	29	60	Контрольный тест
Итого:	**60**	**48**	**108**	

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Наименование модуля, учебного курса	**Год обучения**	**Дата начала обучения**	**Дата окончания обучения**	**Количество учебных недель**	**Количество учебных дней**	**Количество учебных часов**	**Режим занятий**
Модуль 1. Общие сведения об информационной безопасности.	1 год обучения	01.09.2023	29.12.2023	16	16	48 ч.	3 урока 1 раз в неделю по
Модуль 2. Основы персональной кибербезопасности.		08.01.2024	30.05.2024	20	20	60 ч.	3 урока 1 раз в неделю

РАБОЧАЯ ПРОГРАММА УЧЕБНОГО КУРСА «Персональная кибербезопасность»

7-11 классы

Курс «Персональная кибербезопасность» предназначен для обучающихся 7-10 классов.

Курс знакомит обучающихся с основными понятиями информационной безопасности, формирует понимание технологий информационной безопасности и умение применять на практике правила кибербезопасности во всех сферах деятельности.

Модуль 1. Общие сведения об информационной безопасности.

Модуль 2. Основы персональной кибербезопасности.

В результате освоения учебного курса обучающийся должен:

знать:

- Аспекты кибербезопасности, требования к безопасности информации;
- Признаки нарушения целостности программ и данных;
- Меры кибербезопасности для конечных пользователей;
- Нормы сетевого этикета;
- Правовые аспекты защиты киберпростанства.
- **уметь:**
- работать с вычислительной техникой;
- использовать и настраивать антивирусные программы, средства контроля защищенности
- обеспечить безопасность мобильных устройств и сетей Wi-Fi

Тематический план курса

№	Наименование кейса, темы	Количество часов			Формы контроля
		Всего	**Теория**	**Практика**	
Модуль 1. Общие сведения об информационной безопасности.		**29**	**19**	**48**	
Раздел 1. Защита киберпространства как комплекс мероприятий, направленный на обеспечение информационной безопасности.					
1.	Тема 1.1. Компьютерная и информационная безопасность. Аспекты кибербезопасности.	2	1	3	Опрос
2.	Тема 1.2. Обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, критоптографическая защита информации.	4	2	6	Практическая работа
3.	Тема 1.3. Защищенная информационная среда. Защита каналов передачи данных, средства предотвращения утечки информации, защита информации от несанкционированных действий. Средства аутентификации	4	2	6	Практическая работа
4.	Тема 1.4. Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средства резервного копирования и восстановления.	4	2	6	Практическая работа
5.	Тема 1.5. Требования к безопасности информации: сохранение целостности, конфиденциальности, доступности.	2	1	3	Опрос
6.	Тема 1.6. Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения достоверности информации.	4	2	6	Практическая работа
7.	Тема 1.7. Безопасность мобильных устройств в информационных	1	2	3	Практическая работа

	системах. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты).				
8.	Тема 1.8. Угрозы безопасности в сетях Wi-Fi. Методы защиты сетей Wi-Fi.	2	1	3	Лабораторная работа
9.	Тема 1.9. Угрозы информации. Неосторожность пользователя как одна из угроз для информационной безопасности.	2	1	3	Опрос
10.	Тема 1.10. Меры кибербезопасности для конечных пользователей.	2	4	6	Лабораторная работа
11.	Тема 1.11. Киберугрозы Интернета.	2	1	3	Контрольное тестирование по модулю
Модуль 2. Основы персональной кибербезопасности		**31**	**29**	**60**	
Раздел 1. Методы обеспечения безопасности ПК и интернета. Вирусы и антивирусы.					
12.	Тема1.1. Проблемы безопасности инфраструктуры Интернета. Методы защиты.	4	2	6	Опрос
13.	Тема 1.2. Проверка подлинности (аутентификация) в Интернете.	1	2	3	Практическая работа
14.	Тема 1.3. Безопасность при скачивании файлов, просмотре фильмов онлайн. Методы защиты фото и видеоматериалов от копирования в сети.	2	1	3	Практическая работа
15.	Тема 1.4. Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные.	2	1	3	Опрос
16.	Тема 1.5. Источники данных в интернете: почта, сервисы обмена файлами и др. Хранение данных в интернете.	1	2	3	Лабораторная работа
17.	Тема 1.6. Как защитить данные от потерь. Копирование и восстановление. Всегда ли можно спасти свои данные.	2	1	3	Опрос
18.	Тема 1.7. Меры безопасности для пользователя Wi-Fi. Настройка безопасности.	2	4	6	Лабораторная работа
19.	Тема 1.8. Вирусы для мобильных устройств. Методы защиты.	1	2	3	Практическая работа

20.	Тема 1.9. Как развивались вирусы. Как вирусы воздействуют на файлы. Как распознаются вирусы.	2	1	3	Опрос
21.	Тема 1.10. Настройка компьютера для безопасной работы. Ошибки пользователя. (проверка на вирусы)	1	5	6	Практическая работа
22.	Тема 1.11. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.	3	3	6	Практическая работа
23.	Тема 1.12. Сетевой этикет. Реальная и виртуальная личность. Памятка жертвам виртуальной агрессии.	2	1	3	Опрос
Раздел 2. Правовые аспекты защиты киберпространства.					
24.	Тема 2.1. Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, ответственность, меры их предупреждения.	2	1	3	Опрос
25.	Тема 2.2. Как расследуются преступления в сети.	2	1	3	Опрос
26.	Тема 2.3. Ответственность за преступления в сети.	2	1	3	Опрос
27.	Тема 2.4. Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера.	2	1	3	Контрольное тестирование по модулю
	Итого:	**60**	**48**	**108**	

СОДЕРЖАНИЕ КУРСА «Персональная кибербезопасность»

Модуль 1. Общие сведения об информационной безопасности.

Раздел 1. Защита киберпространства как комплекс мероприятий, направленный на обеспечение информационной безопасности

Теория:

Основные понятия и принципы информационной безопасности. Требования к безопасности информации. Признаки нарушения целостности информации. Меры кибербезопасности.

Практика:

− Выполнение практических заданий, лабораторных работ.

Основные методы и формы реализации содержания программы:

–информационно-рецептивный,

–репродуктивный,

–частично-поисковый,

–практический.

Средства обучения:

Программное обеспечение: офисное программное обеспечение.

Форма подведения итогов: Контрольное тестирование.

Модуль 2. Основы персональной кибербезопасности

Раздел 1. Методы обеспечения безопасности ПК и интернета. Вирусы и антивирусы

Теория:

Протоколы маршрутизации сети, система доменных имен, средства маршрутизации, аутентификация. Настройка безопасности сетей Wi-Fi. Безопасность мобильных устройств. Меры личной безопасности при сетевом общении.

Практика:

− Выполнение практических заданий, лабораторных работ.

Основные методы и формы реализации содержания программы:

– информационно-рецептивный,

– репродуктивный,

– частично-поисковый,

– практический.

Средства обучения:

Программное обеспечение: офисное программное обеспечение.

Форма подведения итогов: Контрольное тестирование.

Раздел 2. Правовые аспекты защиты киберпространства.

Теория:

Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, ответственность, меры их предупреждения. Расследования киберпреступлений.

Практика:

− Выполнение практических заданий, лабораторных работ.

Основные методы и формы реализации содержания программы:

– информационно-рецептивный,

– репродуктивный,

– частично-поисковый,

– практический.

Средства обучения:

Программное обеспечение: офисное программное обеспечение.

Форма подведения итогов: Контрольное тестирование

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Во время проведения курса предполагается текущий, промежуточный и итоговый контроль. Промежуточная аттестация обучающихся по данной программе проводится в форме опросов, тестирований, практических работ по каждой теме. Кроме того, проверка результатов освоения программы осуществляется постоянно: после изучения каждого раздела программы, учащиеся контрольные тестирования и лабораторные работы.

Входной контроль – не проводится.

Текущий контроль осуществляется на занятиях в течение всего обучения для отслеживания уровня освоения учебного материала программы.

Формы:

- опрос теоретического материала;
- контрольные тесты.

Промежуточная аттестация проводится с целью выявления уровня освоения программ обучающимися и уровня развития личностных качеств по завершению каждого курса программы.

Формы:

- опрос теоретического материала;
- контрольные тесты;
- практические работы;
- лабораторные работы.

Итоговое оценивание проводится в конце обучения по курсу.

Форма: контрольное тестирование.

Оценка	Результат
Высокий уровень	- Сформированы систематическое знание основных понятий информационной безопасности, - Сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет. - Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию. - Самостоятельно, неординарно решает задачи, способен сам найти свой путь решения. - Проявляет интерес и творческое отношение к изучаемым темам, стремится получить дополнительную информацию. - Может самостоятельно оценить свои возможности в выполнении задания, учитывая изменения известных способов действия. - Проявляет самостоятельность, пунктуальность и ответственность в подготовке к занятиям.
Средний уровень	- Знания в области основных понятий информационной безопасности не систематизированы, хаотичны, частично ошибочные. - Навыки безопасного поведения при работе с компьютерными программами, информацией в сети интернет частично имеются. Иногда нужна помощь. - Интерес возникает к новому материалу, но не к способам его применения на практике. - Может с помощью педагога безопасно работать с информацией, анализировать и обобщать полученную информацию. - Проявляет самостоятельность, но при подготовке к занятиям требуется внешняя стимуляция.
Низкий уровень	- Знания в области основных понятий информационной безопасности отсутствуют. Имеющиеся представления часто ошибочны. - Учащийся не умеет, не пытается и не испытывает потребности в оценке своих действий – ни самостоятельной, ни по просьбе педагога. - Уровень самостоятельности учащихся низкий, при подготовке к занятиям требуется постоянная внешняя стимуляция. - В совместной деятельности не пытается договориться, не может прийти к согласию, настаивает на своем, конфликтует или игнорирует других.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

п/п	Название раздела, темы	Формы учебного занятия	Формы, методы, приемы обучения. Педагогические технологии	Материально-техническое оснащение, дидактико- методический материал	Формы контроля/ аттестации
Модуль 1. Общие сведения об информационной безопасности.					
	Раздел 1. Защита киберпространства как комплекс мероприятий, направленный на обеспечение информационной безопасности.	Комбинированная	Информационно-рецептивный. Репродуктивный. Частично-поисковый. Практический	1. skysmart.py URL: https://edu.skysmart.ru 2. Якласс URL: https://www.yaklass.ru/p/informatika 3. Основы кибербезопасности: учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М.: Дрофа, 2019. — 238, [1] с. — (Российский учебник). 4. Цветкова, М.С. Информационная безопасность. Кибербезопасность. 7–9 классы: учебное пособие /М.С. Цветкова, И.Ю. Хлобыстова. — 2-е изд., пересмотр. — М.: БИНОМ. Лаборатория знаний, 2020 — 64 с.: ил. 5. Наместникова М.С. Информационная безопасность, или на расстоянии одного вируса. 7-9 классы: учеб.пособие для общеобразоват. организаций / М.С. Наместникова. – М.: Просвещение, 2019. – 79 с.: ил. – (Внеурочная деятельность). 6. Макаров С. Прекрасный, опасный, кибербезопасный мир. Все, что важно знать детям и взрослым о безопасности в интернете –М.: 2022. – 568 с.: ил.-	Контрольный тест

Модуль 2. Основы персональной кибербезопасности					
	Раздел 1. Методы обеспечения безопасности ПК и интернета. Вирусы и антивирусы. .	Комбинированная	Информационно-рецептивный. Репродуктивный. Частично-поисковый. Практический	1. Макаров С. Прекрасный, опасный, кибербезопасный мир. Все, что важно знать детям и взрослым о безопасности в интернете –М.: 2022. – 568 с.: ил.- 2. skysmart.py URL: https://edu.skysmart.ru/ 3. Якласс URL: https://www.yaklass.ru/p/informatika 4. Основы кибербезопасности: учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М.: Дрофа, 2019. — 238, [1] с. —	Контрольный тест
	Раздел 2. Правовые аспекты защиты киберпространства	Комбинированная	Информационно-рецептивный. Репродуктивный. Частично-поисковый. Практический	1. Цветкова, М.С. Информационная безопасность. Кибербезопасность. 7–9 классы: учебное пособие /М.С. Цветкова, И.Ю. Хлобыстова. — 2-е изд., пересмотр. — М.: БИНОМ. Лаборатория знаний, 2020 — 64 с.: ил. 2. 149-ФЗ «Об информации, информационных технологиях и о защите информации» 3. 152-ФЗ «О персональных данных» 4. 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	Контрольный тест

КАДРОВОЕ ОБЕСПЕЧЕНИЕ

Преподавание данной программы могут осуществлять педагогические работники, владеющие набором профессиональных навыков в области информационно-коммуникационных технологий, при наличии необходимых компетенций и уровня профильной подготовки.

ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО КУРСУ

Для реализации курса «Персональная кибербезопасность» помещение должно соответствовать следующим характеристикам:

− аудитории, оборудованы интерактивной доской, проектором, ноутбуком.

− каждый обучающийся выполняет практические работы за отдельным компьютером с сохранением результатов в облачном хранилище.

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

1. Перечень литературы, необходимой для освоения программы:

1.1. Перечень литературы, использованной при написании программы:

1. Основы кибербезопасности: учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М.: Дрофа, 2019. — 238, [1] с. — (Российский учебник).

2. Цветкова, М.С. Информационная безопасность. Кибербезопасность. 7–9 классы: учебное пособие /М.С. Цветкова, И.Ю. Хлобыстова. — 2-е изд., пересмотр. — М.: БИНОМ. Лаборатория знаний, 2020 — 64 с.: ил.

3. Наместникова М.С. Информационная безопасность, или на расстоянии одного вируса. 7-9 классы: учеб.пособие для общеобразоват. организаций / М.С. Наместникова. – М.: Просвещение, 2019. – 79 с.: ил. – (Внеурочная деятельность).

4. Макаров С. Прекрасный, опасный, кибербезопасный мир. Все, что важно знать детям и взрослым о безопасности в интернете –М.: 2022. – 568 с.: ил.-.

1.2. Перечень литературы, рекомендованной обучающимся:

1. Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник / Е.К. Баранова, А.В. Бабаш. — М.: РИОР: ИНФРА-М, 2019. — 202 с. — (Среднее про - фессиональное образование)

2. Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2018, 474 с.

3. Макаров С. Прекрасный, опасный, кибербезопасный мир. Все, что важно знать детям и взрослым о безопасности в интернете –М.: 2022. – 568 с.: ил.-.

1.3. Перечень литературы, рекомендованной родителям:

1. Макаров С. Прекрасный, опасный, кибербезопасный мир. Все, что важно знать детям и взрослым о безопасности в интернете –М.: 2022. – 568 с.: ил.-.

1.4 Перечень раздаточного материала:

1. Тематические презентации.

2. Информационное обеспечение

Программное обеспечение:

Операционная система (Windows, Linux, macOS). Офисное программное обеспечение.

2.1 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения программы:

1. https://olimp.edsoo.ru

2. https://edu.skysmart.ru
3. https://www.yaklass.ru/
4. https://uchi.ru
5. https://урок.рф
6. https://education.yandex.ru
7. https://resh.edu.ru