Управление образования города Ростова-на-Дону
Муниципальное бюджетное учреждение
дополнительного образования Железнодорожного района
города Ростова-на-Дону «Дом детского творчества»

ПРИНЯТО
на заседании педагогического совета
совета
Протокол от «22» января 2026 г.
№ 3

УТВЕРЖДАЮ
Директор МБУ ДО ДДТ
Подписан: Андреева Наталья Николаевна
DN: C=RU, OU=директор, O=МБУ ДО ДДТ, CN=Андреева Наталья Николаевна, E=ddtrostov@yandex.ru
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: 344101 г.Ростов-на-Дону,ул.Верещагина,10
Дата: 2026.01.22 14:47:11+03'00'
Андреева Н.Н.
Приказ от «22» января 2026 г.
№13

СОГЛАСОВАНО
на заседании методического
совета
Протокол от «22» января 2026 г.
№3

ДОПОЛНИТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА
социально-гуманитарной направленности
«Цифровая безопасность»

Подвид программы: сетевая
Уровень программы: стартовый
Целевая группа (возраст):от 7 до 10 лет
Срок реализации: 1 год, 72 часа
Форма реализации программы: очная
Условия реализации программы:
социальный сертификат
Разработчик: Вещева Юлия Олеговна
старший методист

г. Ростов-на-Дону
2026

Оглавление

Раздел 1. Комплекс основных характеристик образования.

1.1. Пояснительная записка.

Нормативно-правовая база

1. Конституция РФ (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
2. Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 28.02.2025) «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 11.03.2025, далее - ФЗ №273).
3. Распоряжение Правительства РФ от 31.03.2022 г. № 678-р «Концепция развития дополнительного образования детей до 2030 года» (далее - Концепция).
4. Федеральный закон РФ от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» (с изменениями от 29.12.2022г.).
5. Указ президента РФ от 07.05.2024 г. №309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года».
6. Указ Президента РФ от 09.11.2022 №809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей».
7. Приказ Министерства просвещения РФ от 27.06.2022 г. № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»
8. Приказ Министерства просвещения РФ от 03.09.2019 № 467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей» (в редакции от 21.04.2023г.).
9. Постановление Главного государственного санитарного врача РФ от 28.09.2020 г. № 28 «Об утверждении санитарных правил СП 2.4.3648-20.
10. Постановление Главного государственного санитарного врача Российской Федерации от 28.01.2021 № 2 «Об утверждении санитарных правил и норм СанПиН 1.2.368521 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания»
11. Приказ Управления образования от 23.08.2023 № УОПР-643 «О проведении независимой оценки качества дополнительных общеобразовательных программ образовательных организаций в городе Ростове-на-Дону».
12. Приказ Министерств общего и профессионального образования Ростовской области от 01.08.2023 г. № 718 «О проведении независимой оценки качества дополнительных общеобразовательных программ в Ростовской области».
13. Приказ Управления образования от 16.11.2023 г. № УОПР-982 «Об утверждении Требований к условиям и порядку оказания муниципальной услуги в социальной сфере «Реализация дополнительных общеразвивающих программ (общественной экспертизы) на соответствие Требованиям к условиям и порядку оказания муниципальной услуги «реализация дополнительных общеразвивающих программ» в соответствии с социальными сертификатами.
14. Приказ Минобразования РО №136 от 14.02.2024г. «О внесении изменений в приказ минобразования Ростовской области от 01.08.2023 № 718».

15. Приказ Минобразования РО №724 от 03.08.2023г. «Об утверждении Требований к условиям и порядку оказания государственной услуги в социальной сфере „Реализация дополнительных общеразвивающих программ“ в Ростовской области».
16. Письмо Министерства Просвещения Российской Федерации № АБ-3936/06 от 29.09.2023 «Методические рекомендации по формированию механизмов обновления содержания, методов и технологий обучения в системе дополнительного образования детей»
17. Письмо Министерства образования и науки РФ от 18 ноября 2015 г. № 09-3242 «О направлении информации» (вместе с «Методическими рекомендациями по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы)»)
18. Приказ Министерства общего и профессионального образования Ростовской области от 03.08.2023 года № 724 «Об утверждении Требований к условиям и порядку оказания государственной услуги в социальной сфере «Реализация дополнительных общеразвивающих программ»».
19. Методические рекомендации по разработке дополнительных общеразвивающих программ, в том числе в части интеграции с учебными предметами «Труд (технология)», «Музыка», «Изобразительное искусства», «Физическая культура», утверждены Министерством просвещения РФ от 23 января 2026 года.
20. Приказ Управления образования города Ростова-на-Дону от 21 февраля 2024 года №УОПР/158 «О внесении изменений в приказ Управления образования города Ростова-на-Дону от 15 декабря 2023 года №УОПР/1100».
21. Методические рекомендации по оформлению структурных элементов дополнительных общеразвивающих программ, утвержденные на заседании методического совета ГАУ ДПО РО «Институт развития образования», протокол от 29.03.2024 г. № 3.
22. Письмо Минобразования РО ГАУ ДПО РО ИРО от 09.04.2024 Рекомендации по оформлению и содержанию структурных элементов, Пр. от 29.03.2024 г.№3.

Направленность программы: техническая.

Актуальность программы. Сетевое взаимодействие обеспечивает широкий охват обучающихся разных образовательных организаций, равный доступ к современному компьютерному оборудованию и единое качество дополнительного образования, что соответствует задачам национального проекта «Образование» в части развития инфраструктуры и повышения доступности дополнительного образования для детей. Программа отвечает социальному запросу родителей, заинтересованных в системном обучении детей правилам кибербезопасности, и согласуется с требованиями федеральных нормативных документов, включая Концепцию информационной безопасности детей (распоряжение Правительства РФ от 28.04.2023 № 1105-р) и Федеральную образовательную программу начального общего образования (приказ Минпросвещения России от 18.05.2023 № 370), предписывающие формирование

цифровой грамотности с раннего школьного возраста. обусловлена критическим разрывом между активным вовлечением обучающихся в цифровую среду и отсутствием у них сформированных навыков безопасного поведения в сети. В этом возрасте обучающиеся получают первые самостоятельные устройства, начинают пользоваться образовательными платформами и общаться в мессенджерах, однако в силу психофизиологических особенностей (доверчивость, недостаточный критический кругозор) они наиболее уязвимы перед киберугрозами. Согласно статистике, значительная часть обучающихся сталкивается с опасными знакомствами в сети, переходом на фишинговые сайты и риском утечки персональных данных, что вызывает обоснованную тревогу у родителей (59% взрослых выражают обеспокоенность влиянием гаджетов на безопасность детей). Программа напрямую отвечает на запрос родителей**,** которые, согласно опросам, в первую очередь опасаются, что ребенок столкнется с мошенниками, попадет под влияние деструктивных сообществ или станет жертвой буллинга в сети, но при этом не имеют возможности системно обучить его цифровой гигиене. Программа отвечает на социальный запрос общества и полностью соответствует государственной политике в сфере образования: она реализует положения Концепции информационной безопасности детей (распоряжение Правительства РФ от 28.04.2023 № 1105-р), которая определяет обучение безопасному поведению в интернете как приоритетную задачу, и интегрируется с требованиями Федеральной образовательной программы начального общего образования**,** предписывающей формирование основ цифровой грамотности и критического отношения к информации уже на уровне начальной школы. Кроме того, содержание программы базируется на принципах Федерального закона № 436-ФЗ «О защите детей от информации...» адаптируя их правовые нормы в доступную для младших школьников форму. Таким образом, программа не только восполняет дефицит системных знаний о кибербезопасности, но и создаёт фундамент для дальнейшего безопасного использования цифровых технологий в рамках реализации национальных целей по формированию безопасной информационной среды для обучающихся.

Отличительные особенности программы, новизна:

Программа является **модифицированной**, реализуется в сетевой форме. Так как программа реализуется в сетевой форме, она позволяет объединить кадровый потенциал **базовой организации** Муниципальное бюджетное учреждение дополнительного образования Железнодорожного района города Ростова-на-Дону «Дом детского творчества» с материально-техническими ресурсами **образовательного учреждения-партнера**: МБОУ «Школа № 83 имени Героя Российской Федерации Казанцева В.Г.», (МБОУ "**Школа № 83**"). Основной отличительной особенностью программы от аналогичных программ является её реализация **в сетевой форме,** что позволяет объединить кадровые ресурсы учреждения дополнительного образования и материально-техническую базу нескольких общеобразовательных школ.

Сетевое взаимодействие в программе построено на принципе взаимодополнения ресурсов базовой организации и образовательного

учреждения-партнера. Муниципальное бюджетное учреждение дополнительного образования Железнодорожного района города Ростова-на-Дону «Дом детского творчества» выступает базовой организацией, обеспечивая реализацию программы квалифицированными педагогическими кадрами, методическое сопровождение и организацию воспитательной работы. Организация-партнер – общеобразовательная школа – предоставляет материально-техническую базу: компьютерный класс, оснащенный современным оборудованием и программным обеспечением, необходимым для проведения практических занятий по цифровой безопасности. Такая модель позволяет эффективно использовать имеющиеся ресурсы, обеспечивает доступность программы для обучающихся разных образовательных учреждений и создает единое образовательное пространство.

Реализация программы осуществляется на основании договора о сетевом взаимодействии, в которых закреплены распределение обязанностей, порядок использования ресурсов и ответственность сторон.

Способ реализации сетевого взаимодействия, обязательства организаций партнеров: МБУ ДО ДДТ – предоставляет педагогические кадры отвечает за организацию образовательного процесса, осуществляет контроль за его реализацией, проводит промежуточный контроль и подводит итоги реализации программы, отвечает за методическое сопровождение образовательной программы, обеспечение методическими материалами.

МБОУ "Школа № 83", является базой для проведения занятий, мероприятий; предоставляет материально-техническое обеспечение (помещение, оборудование, материалы и т.д.).

Реализация программы осуществляется на основании договора о сетевом взаимодействии, в котором закреплены распределение обязанностей, порядок использования ресурсов и ответственность сторон (Приложение 6).

Программа является **модифицированной.** При разработке программы был проведен анализ существующих методических материалов в сфере цифровой безопасности. В качестве аналогов можно рассматривать программу «Кибербезопасность», автор Авдеев Никита Юрьевич, г. Электросталь Московской области), а также типовые модули по информационной безопасности, включенные в курс «Информатика» для начальной школы и различные внеурочные разработки по защите от киберугроз. Большинство существующих программ либо ориентированы на изучение технических аспектов (защита устройств, настройки конфиденциальности) и рассчитаны на подростков, либо носят ознакомительный характер и фрагментарно затрагивают вопросы безопасности в общем курсе информатики.

Отличает программу от аналогичных программ **интеграция с родительским запросом.** Впервые в структуру программы (в отличие от существующих аналогов) заложен механизм обратной связи с семьей. Содержание программы предполагает совместные детско-родительские квизы и памятки, что превращает обучение из изолированного курса в часть семейной системы воспитания цифровой культуры.

Специфика данной программы предполагает наличие таких педагогических технологий как **сценарный подход и геймификация:** занятия строятся по принципу интерактивного квеста или детективного расследования («Агенты кибербезопасности»), где каждый обучающийся не просто слушатель, а активный участник, принимающий решения в смоделированных опасных ситуациях.

Новизна. Новизна программы заключается в реализации сетевой формы взаимодействия, объединяющей кадровый потенциал учреждения дополнительного образования и материально-техническую базу нескольких общеобразовательных школ, что обеспечивает доступность, эффективность и единое качество обучения цифровой безопасности для детей из разных образовательных организаций. Новизной программы также является ее возрастная адаптивность. В отличие от программы Авдеева Н.Ю. и других технически ориентированных аналогов, данная программа учитывает психологические особенности детей 7–10 лет. Сложные темы (фишинг, кибербуллинг, персональные данные) адаптированы через игровые метафоры («Цифровой светофор», «Защита личного домика»), что делает материал доступным для обучающихся без потери смысловой глубины.

Новым является ее социально-эмоциональный акцент и заключается в смещении фокуса с сугубо технической защиты устройства на защиту личности ребенка.

Нововведения в диагностике: традиционное тестирование знаний заменено на мониторинг поведенческих реакций. Входная диагностика и подведение итогов реализации программы проводятся в формате анализа решения проблемных кейсов и наблюдения за действиями обучающихся в игровых симуляторах, что позволяет оценить не объем заученной информации, а сформированность навыка безопасного поведения.

Педагогическая целесообразность. Педагогическая целесообразность программы заключается в том, что освоение её содержания обучающимися способствует формированию ответственного цифрового гражданства, основ патриотизма и уважения к информационному суверенитету своей страны. Обучающиеся не просто осваивают правила безопасного поведения, но и осознают ценность персональных данных как части личного и государственного достояния, учатся противостоять деструктивному контенту и информационным угрозам, направленным на разобщение общества.

Занятия проводятся в разновозрастных группах (7–10 лет), что создает уникальную воспитательную среду. Ведущую роль играет межвозрастное взаимодействие, связующим звеном которого выступает игровая и проектная деятельность. Обучающиеся младшего школьного возраста, глядя на более старших товарищей, быстрее осваивают модели этичного поведения в сети, а старшие, помогая младшим, закрепляют собственные навыки цифровой гигиены и развивают чувство ответственности за общую цифровую безопасность коллектива. Такой подход позволяет моделировать реальные социальные связи, существующие в цифровой среде, и учит детей грамотно выстраивать коммуникацию независимо от возраста собеседника.

Адресат программы: обучающиеся в возрасте от 7 до 10 лет.

Объем и срок освоения программы: 72 часа, 1 год.

Режим занятий: 1 раз в неделю по 2 часа.

Уровень сложности содержания программы: стартовый.

Форма обучения: очная.

Форма организации образовательного процесса: групповая. Наполняемость группы и условия комплектования: от 10 до 12 обучающихся. Группы комплектуются по заявлению родителей, принимаются все желающие, без предварительного отбора.

Виды занятий: практические, теоретические, комбинированные.

Перечень форм подведения итогов программы: защита проекта, решение проблемных кейсов.

Особенности организации образовательного процесса: при разработке программы учитываются возрастные психофизиологические особенности обучающихся 7–10 лет, что определяет специфику преподавания программы. В этом возрасте у обучающихся преобладает наглядно-образное мышление и конкретность восприятия, программе сложные абстрактные понятия (фишинг, кибербуллинг) заменяются визуальными образами и моделируются через конкретные жизненные ситуации. Обучающиеся младшего школьного возраста отличаются доверчивостью и авторитарностью мышления, склонны доверять незнакомцам в сети, поэтому программа делает акцент на отработку навыков критического восприятия информации через специальные игровые упражнения. В силу повышенной эмоциональности и эгоцентризма обучающиеся остро воспринимают критику, но не всегда осознают последствия своих действий для других, что компенсируется включением в занятия ролевых игр, развивающих эмпатию и понимание чувств собеседника. Учитывая преобладание непроизвольного внимания и быструю утомляемость, структура занятий строится на частой смене видов деятельности (игра, просмотр, обсуждение, практикум), что позволяет удерживать интерес и предотвращать переутомление. Поскольку игра остается ведущим видом деятельности наряду с учебой, программа активно использует сюжетно-ролевые игры и квесты, где каждый обучающийся получает значимую роль, что удовлетворяет его потребность в признании. Наконец, с учетом становления произвольности поведения и импульсивности реакции в стрессовых ситуациях, программа через многократное повторение простых алгоритмов (по типу «цифровых правил светофора») доводит навыки безопасного поведения у обучающихся до автоматизма.

Программа не предназначена для детей-инвалидов и детей с ограниченными возможностями здоровья.

1.2. Цель и задачи.

Цель: создание условий для формирования у обучающихся осознанного и ответственного отношения к личной безопасности в цифровом пространстве, развитие навыков распознавания киберугроз и противодействия им, а также воспитание культуры позитивного и этичного общения в сети.

Задачи:

развивающие:

- развитие логического мышления и способности анализировать ситуации, связанные с цифровыми рисками;
- развитие внимания и наблюдательности при работе с информацией в сети (умение замечать «опасные сигналы»);
- развитие памяти через запоминание алгоритмов безопасного поведения и правил цифровой гигиены;
- развитие воображения и творческих способностей через создание проектов (памятки, плакаты, цифровые истории) на тему безопасности;
- развитие коммуникативных навыков и умения выражать свою позицию в процессе обсуждения и ролевых игр;
- развитие волевых качеств (умение сказать «нет», выйти из опасной ситуации, обратиться за помощью).

воспитательные:

- воспитание ответственного отношения к личной информации и уважения к приватности других людей;
- формирование ценностного отношения к доброжелательному и этичному общению, нетерпимости к проявлениям кибербуллинга;
- воспитание цифрового патриотизма и понимания важности защиты информационного пространства своей страны;
- формирование навыков рефлексии и самооценки собственного поведения в цифровой среде;
- воспитание самостоятельности и умения принимать ответственные решения в ситуациях онлайн-риска;
- формирование установки на обращение за помощью к взрослым в сложных или опасных ситуациях в сети.

обучающие:

- знакомство обучающихся с основными правилами цифровой гигиены и безопасного использования сети Интернет;
- формирование представлений о видах киберугроз (фишинг, кибербуллинг, вредоносные программы, нежелательный контент) и способах их распознавания;
- освоение алгоритмов защиты персональных данных и безопасного создания цифрового профиля (пароли, аватары, настройки конфиденциальности);
- обучение применению правил этичного и безопасного общения в мессенджерах, социальных сетях и онлайн-играх;
- формирование навыков критического анализа информации и умения отличать достоверные источники от недостоверных.

1.3. Содержание программы.

1.3.1. Учебный план

Таблица 1.

№ п/п	Название разделов и тем	Количество часов			Форма контроля, аттестации
		Всего	Теория	Практика	
1	**Раздел 1. Введение в цифровую безопасность**	**10**	**4**	**6**	
1.1	Вводное занятие. Инструктаж по технике безопасности. Стартовая педагогическая диагностика	2	1	1	Тестирование (входная диагностика)
1.2	Что такое Интернет: возможности и опасности	2	1	1	Устный опрос
1.3	Компьютер и устройство: правила безопасного использования	2	1	1	Практическое задание
1.4	Мои цифровые помощники (браузеры, поисковики, приложения)	2	1	1	Наблюдение
1.5	Создание памятки «Правила безопасного старта»	2	0	2	Творческая работа
2	**Раздел 2. Персональные данные и цифровой профиль**	**12**	**4**	**8**	
2.1	Что такое персональные данные? Личное и публичное	2	1	1	Беседа

№ п/п	Название разделов и тем	Количество часов			Форма контроля, аттестации
2.2	Пароли: секреты надежной защиты	2	1	1	Практикум по созданию паролей
2.3	Аватар, никнейм и профиль: безопасное представление себя в сети	2	1	1	Творческое задание
2.4	Настройки конфиденциальности в играх и приложениях	2	1	1	Практическая работа на ПК
2.5	Что нельзя публиковать в соцсетях? Разбор ситуаций	2	0	2	Анализ кейсов
2.6	Квест «Мой цифровой двойник»	2	0	2	Анализ участия в квесте
3	**Раздел 3. Безопасное общение в цифровой среде**	**14**	**4**	**10**	
3.1	Правила этикета в мессенджерах и соцсетях	2	1	1	Ролевая игра
3.2	Друзья и незнакомцы в сети: как отличить и не ошибиться	2	1	1	Анализ ситуаций
3.3	Что такое кибербуллинг? Как распознать и что делать	2	1	1	Беседа, тренинг
3.4	Если обижают в сети: алгоритмы помощи и поддержки	2	0	2	Ролевая игра
3.5	Добрые и злые сообщения: учимся различать намерения	2	1	1	Практикум

№ п/п	Название разделов и тем	Количество часов			Форма контроля, аттестации
3.6	Создание комикса «История одной переписки». Игра-тренинг «Безопасный чат».	2	0	2	Творческий проект
3.7	Новогодний квест «Агенты кибербезопасности спешат на помощь»	2	0	2	Анализ участия в квесте
4	**Раздел 4. Информационная безопасность: учимся думать критически**	**12**	**4**	**8**	
4.1	Правда и ложь в Интернете: как проверить информацию	2	1	1	Практикум с поисковиками
4.2	Фишинг: опасные ссылки и подозрительные письма	2	1	1	Тренинг на тренажере
4.3	Вирусы и вредоносные программы: что это и как защититься	2	1	1	Практическая работа
4.4	Реклама и ловушки: учимся говорить «нет»	2	1	1	Анализ сайтов
4.5	Создание памятки «Проверяй, прежде чем нажать»	2	0	2	Творческая работа
4.6	Итоговое занятие по модулю: игра-соревнование «Детективы информации»	2	0	2	Командная игра

№ п/п	Название разделов и тем	Количество часов			Форма контроля, аттестации
5	**Раздел 5. Цифровое здоровье и безопасность**	**10**	**4**	**6**	
5.1	Время за компьютером: сколько можно и как не навредить себе	2	1	1	Беседа, составление режима
5.2	Осанка, зрение и физминутки: заботимся о здоровье	2	1	1	Практикум (физминутки)
5.3	Игры: полезные, бесполезные и опасные	2	1	1	Анализ игр
5.4	Как не попасть в зависимость от гаджетов	2	1	1	Тренинг
5.5	Создание плаката «Здоровый цифровой образ жизни»	2	0	2	Творческая работа
6	**Модуль 6. Итоговая аттестация и проектная деятельность**	**14**	**2**	**12**	
6.1	Подготовка итогового проекта (выбор темы, сбор материалов)	4	1	3	Консультация
6.2	Создание итогового проекта (презентация, памятка, плакат, комикс)	4	0	4	Самостоятельная работа
6.3	Защита итоговых проектов	4	1	3	Защита проекта

№ п/п	Название разделов и тем	Количество часов			Форма контроля, аттестации
6.4	Заключительное занятие	2	0	2	Решение проблемных кейсов
	ИТОГО:	**72**	**22**	**50**	

1.3.2. Содержание учебного плана.

Раздел 1. Введение в цифровую безопасность (10 ч.)

Тема 1.1. Вводное занятие. Стартовая педагогическая диагностика (2 ч.). *Теория (1 ч.).* Инструктаж по технике безопасности. Знакомство с программой «Цифровая безопасность». Правила поведения и техника безопасности. Понятие о цифровой безопасности: зачем нужно защищать себя в Интернете. Введение в игровую сюжетную линию: мы — команда защитников цифрового города. *Практика (1 ч.).* Стартовая диагностика: тестирование в игровой форме (разбор простых ситуаций «Безопасно — опасно»). Анкетирование «Мой цифровой мир».

Тема 1.2. Что такое Интернет: возможности и опасности (2 ч.). *Теория (1 ч.).* Интернет как «цифровой океан»: полезные ресурсы для учёбы и игр, общение с друзьями. Сказочная метафора «Цифровой лес»: добрые жители (полезные сайты) и опасные хищники (мошенники, вирусы). *Практика (1 ч.).* Интерактивная игра «Путешествие по цифровому океану»: на игровых карточках обучающиеся распределяют ситуации на «безопасные» и «опасные», учатся видеть первые признаки угрозы.

Тема 1.3. Компьютер и устройство: правила безопасного использования (2ч.). *Теория (1 ч.).* Общий вид компьютера: системный блок, монитор, клавиатура, мышь. Назначение основных устройств. Метафора «Тело компьютера»: процессор — это «мозг», память — «блокнот», монитор — «глаза». Правила безопасной работы за компьютером (осанка, расстояние до экрана, перерывы). *Практика (1 ч.).* Тренировочные упражнения: игра «Собери компьютер» (на карточках или в программе). Составление короткого рассказа с ошибками «Мой компьютер» с последующим коллективным исправлением.

Тема 1.4. Мои цифровые помощники (браузеры, поисковики, приложения)(2ч.). *Теория (1 ч.).* Что такое браузер — «ворота в Интернет». Поисковики: как они помогают находить информацию. Приложения: полезные и игровые. Метафора «Цифровые инструменты». *Практика (1 ч.).* Практическая работа в компьютерном классе: открытие браузера, переход на безопасный детский сайт (по образцу педагога, знакомство с интерфейсом поисковика. Упражнение «Найди по описанию».

Тема 1.5. Создание памятки «Правила безопасного старта» (2 ч.). *Практика (2 ч.).* Творческая групповая работа: создание памятки-плаката (на бумаге или в простом графическом редакторе) с основными правилами безопасного начала работы за компьютером. Презентация памяток друг другу.

Раздел 2. Персональные данные и цифровой профиль (12 ч.)

Тема 2.1. Что такое персональные данные? Личное и публичное (2 ч.). *Теория (1 ч.).* Понятие «персональные данные» в доступной форме: информация, которая позволяет нас узнать (имя, фамилия, адрес, фото). Метафора «Цифровой домик»: есть комната для всех (гостиная) и своя комната (только для себя и близких). Что можно рассказывать о себе всем, а что — только семье. *Практика (1 ч.).* Игра с карточками «Можно — нельзя»: обучающиеся

распределяют информацию (имя, адрес, номер школы, любимый цвет, фото) на две группы.

Тема 2.2. Пароли: секреты надежной защиты (2 ч.).

Теория (1 ч.). Зачем нужен пароль. Пароль как «ключ от цифрового домика». Какие пароли бывают (простые, сложные). Почему нельзя использовать один пароль везде и делиться им с друзьями. Правила создания надежного пароля (длина, буквы, цифры, символы).

Практика (1 ч.). Практикум «Придумай надежный пароль» (на бумаге, без ввода в реальные аккаунты). Игра-соревнование «Чей пароль сложнее?». Анализ сказочных ситуаций («Волк и семеро козлят» в цифровом мире — козлята открыли дверь незнакомцу).

Тема 2.3. Аватар, никнейм и профиль: безопасное представление себя в сети(2ч.).

Теория (1 ч.). Что такое аватар и никнейм. Почему не стоит ставить свое реальное фото на аватар в играх и соцсетях (метафора «Маска супергероя»). Как выбрать безопасный никнейм (без фамилии и года рождения). Какая информация в профиле безопасна, а какая опасна.

Практика (1 ч.). Творческое задание: придумать себе безопасный никнейм и нарисовать аватар (или создать в простом графическом редакторе), не используя реальные фото и данные.

Тема 2.4. Настройки конфиденциальности в играх и приложениях (2 ч.).

Теория (1 ч.). Понятие «настройки приватности»: кто может видеть твою страницу, писать тебе, добавлять в друзья. Метафора «Забор вокруг цифрового домика»: настройки защищают наш домик от чужих.

Практика (1 ч.). Практическая работа на компьютере (на учебных тренажерах, имитирующих интерфейс соцсети или игры): совместно с педагогом разбираем, где находятся настройки и какие параметры лучше выбрать (например, «только друзья»).

Тема 2.5. Что нельзя публиковать в соцсетях? Разбор ситуаций (2 ч.).

Практика (2 ч.). Работа в малых группах: анализ ситуаций (карточки с историями). Обучающиеся обсуждают, что герои историй сделали неправильно, что опубликовали зря и к каким последствиям это привело. Коллективная выработка правил «Никогда не публикуй...».

Тема 2.6. Итоговое занятие по модулю: квест «Мой цифровой двойник» (2ч.).

Практика (2 ч.). Командная игра-квест. Обучающиеся выполняют задания на станциях: «Собери пароль», «Настрой приватность», «Выбери безопасный аватар». Цель — защитить своего «цифрового двойника» от злоумышленников.

Раздел 3. Безопасное общение в цифровой среде (14 ч.)

Тема 3.1. Правила этикета в мессенджерах и соцсетях (2 ч.).

Теория (1 ч.). Что такое «сетевой этикет» или «цифровые правила вежливости». Почему важно здороваться, прощаться, не писать капслоком (метафора «крик в чате»), уважать чужое время. Отличие общения в реальной жизни и в сети (не видно интонаций, эмоций).

Практика (1 ч.). Ролевая игра «Вежливый разговор»: Обучающиеся в парах

разыгрывают диалоги в мессенджере (на карточках или в учебном чате), учатся правильно выражать мысли и эмоции (через смайлы, слова).

Тема 3.2. Друзья и незнакомцы в сети: как отличить и не ошибиться (2 ч.). *Теория (1 ч.).* Кто такой «друг» в реальной жизни и кто такой «друг» в сети. Почему не все, кто пишет «привет, давай дружить», на самом деле хотят дружить. Метафора «Волк в овечьей шкуре». Признаки опасного незнакомца (просит фото, адрес, встретиться, прислать пароль). *Практика (1 ч.).* Анализ ситуаций на карточках «Новый друг в сети»: обучающиеся учатся распознавать подозрительные сообщения и формулировать отказ. Отработка фраз-отказов.

Тема 3.3. Что такое кибербуллинг? Как распознать и что делать (2 ч.). *Теория (1 ч.).* Понятие «кибербуллинг» (травля в сети) в доступной форме: обидные комментарии, злые сообщения, исключение из игры, насмешки. Почему обидчики в сети чувствуют себя безнаказанными. Эмпатия: как чувствует себя тот, кого обижают. *Практика (1 ч.).* Беседа-обсуждение с элементами тренинга: просмотр коротких мультфильмов или социальных роликов на тему буллинга, обсуждение чувств героев. Упражнение «Как поддержать друга».

Тема 3.4. Если обижают в сети: алгоритмы помощи и поддержки (2 ч.). *Практика (2 ч.).* Ролевая игра «Стоп-обида»: обучающиеся проигрывают ситуации, где один обижает, другой обижается, третий — наблюдатель. Отработка алгоритма: 1) не отвечай обидчику, 2) сохрани доказательства (скриншот), 3) заблокируй, 4) расскажи взрослому. Создание общего «Правила четырех шагов».

Тема 3.5. Добрые и злые сообщения: учимся различать намерения (2 ч.). *Теория (1 ч.).* Как слова могут ранить даже без картинок. Учимся «читать между строк»: почему одно и то же сообщение может быть шуткой для друга и обидой для другого. Понятие троллинга (провокации). Как не поддаваться на провокации. *Практика (1 ч.).* Практикум: на экране или карточках показываются разные сообщения, обучающиеся определяют, какое из них доброе, какое злое, а какое — провокация. Учатся не отвечать на провокации (игра «Лед и пламя» — сохраняем спокойствие).

Тема 3.6. Создание комикса «История одной переписки» (2 ч.).. *Практика (2 ч.).* Творческая групповая работа: создание комикса (на бумаге или в цифровом редакторе), в котором отражены правила безопасного общения, распознавание незнакомцев, противодействие буллингу. Презентация комиксов. Игра-тренинг «Безопасный чат». Игра-тренинг: моделируется учебный чат, в котором обучающиеся общаются, но появляются «провокаторы» (задания от педагога). Обучающиеся должны применить все знания: соблюдать этикет, не вестись на провокации, не делиться личным, распознавать «троллей».

Тема 3.7. *Практика (2 ч).* **Новогодний квест «Агенты кибербезопасности спешат на помощь».** Командная игра, передвижение по станциям, в ходе которой обучающиеся 7–10 лет выполняют задания, проверяющие знания и умения, полученные за первое полугодие: устройство компьютера, защита

персональных данных, создание надежных паролей, правила общения с незнакомцами в сети и сетевой этикет. Передвигаясь по станциям («Собери компьютер», «Цифровой домик», «Пароль для Деда Мороза», «Агент под прикрытием», «Вежливый чат»), команды собирают фрагменты кода, чтобы спасти «Новогодний огонек».

Раздел 4. Информационная безопасность: учимся думать критически (12 ч.)

Тема 4.1. Правда и ложь в Интернете: как проверить информацию (2 ч.).

Теория (1 ч.). Почему не всему, что написано в Интернете, можно верить. Метафора «Сломанный телефон» в цифровом мире. Кто и зачем распространяет ложную информацию. Первые признаки недостоверной информации (слишком страшно, слишком выгодно, нет подтверждений).

Практика (1 ч.). Практикум с поисковиками: обучающимся даются два утверждения (например, «Правда ли, что жираф спит 2 часа?»). Учимся сравнивать информацию из разных источников, искать подтверждение на проверенных сайтах (под контролем педагога).

Тема 4.2. Фишинг: опасные ссылки и подозрительные письма (2 ч.).

Теория (1 ч.). Понятие «фишинг» (ловля рыбы) — мошенники «ловят» наши пароли и данные. Что такое подозрительные письма («Вы выиграли миллион!», «Ваш аккаунт взломали, перейдите по ссылке»). Метафора «Червивое яблоко» — красивое снаружи, опасно внутри. Опасные ссылки: нельзя нажимать на незнакомые ссылки.

Практика (1 ч.). Тренинг на учебном тренажере (имитация почтового ящика): обучающиеся учатся отличать настоящие письма от фишинговых, находить признаки обмана (ошибки, странный адрес отправителя, угрозы или слишком заманчивые предложения).

Тема 4.3. Вирусы и вредоносные программы: что это и как защититься (2ч.).

Теория (1 ч.). Что такое компьютерные вирусы (по аналогии с вирусами простуды — заражают компьютер и мешают ему работать). Как вирус может попасть в компьютер (через игры, файлы, флешки, ссылки). Антивирус — «доктор» для компьютера. Правила: не скачивай игры с непонятных сайтов, не открывай подозрительные файлы.

Практика (1 ч.). Практическая работа: на учебном компьютере (в безопасной среде) знакомство с понятием «расширение файла»: учимся отличать картинку от программы. Игра «Найди опасный файл» (среди иконок найти подозрительные).

Тема 4.4. Реклама и ловушки: учимся говорить «нет» (2 ч.).

Теория (1 ч.). Реклама в Интернете: что это такое и зачем она нужна. Почему нельзя верить всей рекламе («Бесплатно!», «Только сегодня!»). Навязчивые кнопки, всплывающие окна, ложные награды в играх. Учимся говорить «нет» и закрывать подозрительные окна.

Практика (1 ч.). Анализ сайтов (специально подобранных педагогом) с безопасной рекламой или ее имитацией. Упражнение «Найди ловушку»: обучающиеся ищут на макетах страниц элементы, которые пытаются обмануть пользователя.

Тема 4.5. Создание памятки «Проверяй, прежде чем нажать» (2 ч.). *Практика (2 ч.).* Творческая работа: создание памятки-инфографики (на бумаге или в простом редакторе) с главными правилами: «Не нажимай на незнакомые ссылки», «Проверяй информацию», «Не верь всему, что пишут», «Советуйся со взрослыми».

Тема 4.6. Итоговое занятие по модулю: игра-соревнование «Детективы информации»(2ч.).

Практика (2 ч.). Командная игра-соревнование: команды получают «дела» (кейсы с подозрительными письмами, ссылками, новостями) и должны определить, правда это или ложь, найти признаки фишинга, предложить правильные действия. Побеждает команда, раскрывшая больше «преступлений».

Раздел 5. Цифровое здоровье и безопасность (10 ч.)

Тема 5.1. Время за компьютером: сколько можно и как не навредить себе(2ч.).

Теория (1 ч.). Почему важно ограничивать время за экраном (переутомление, глаза, сон, прогулки). Возрастные нормы работы за компьютером. Метафора «Цифровой таймер»: наши глаза и голова тоже устают. Признаки усталости.

Практика (1 ч.). Беседа с элементами составления индивидуального режима дня (сколько времени можно играть, делать уроки за компьютером, отдыхать). Составление памятки «Мой экранный день».

Тема 5.2. Осанка, зрение и физминутки: заботимся о здоровье (2ч.).

Теория (1 ч.). Правильная поза за компьютером: как сидеть, чтобы не болела спина. Гимнастика для глаз: зачем она нужна. Профилактика «компьютерной усталости».

Практика (1ч.). Практикум: разучивание комплекса упражнений физминутки и гимнастики для глаз. Каждое занятие теперь начинается с «минутки здоровья» (выполнения разученных упражнений).

Тема 5.3. Игры: полезные, бесполезные и опасные (2ч.).

Теория (1 ч.). Какие бывают игры: развивающие, развлекательные, игры с общением. Как отличить полезную игру от пустой траты времени. Признаки опасных игр (требуют личные данные, толкают на опасные поступки в реальности, требуют денег).

Практика (1 ч.). Анализ игр (названия и краткие описания на карточках). Обучающиеся распределяют игры на три группы: «полезные», «бесполезные», «опасные» и объясняют свой выбор.

Тема 5.4. Как не попасть в зависимость от гаджетов (2ч.).

Теория (1 ч.). Что такое «зависимость от гаджетов» (когда не можешь оторваться от телефона/компьютера). Признаки зависимости (все время хочется играть, забрасываешь уроки, не гуляешь, ссоришься с родителями из-за времени). Как найти баланс: учеба, спорт, прогулки, живое общение.

Практика (1 ч.). Тренинг «Мои увлечения помимо гаджетов»: обучающиеся рассказывают, что они любят делать в реальном мире. Упражнение «Идеальный день»: составление расписания дня, где есть место и гаджетам, и другим занятиям.

Тема 5.5. Создание плаката «Здоровый цифровой образ жизни» (2 ч.). *Практика (2 ч.).* Творческая групповая работа: создание плаката (на бумаге или в цифровом формате), призывающего к здоровому использованию гаджетов, с правилами и яркими образами. Размещение плакатов в классе или школе.

Раздел 6. Итоговая аттестация и проектная деятельность (14 ч.)

Тема 6.1. Подготовка итогового проекта (выбор темы, сбор материалов) (4ч.). *Теория (1 ч.).* Знакомство с темами проектов, требованиями к работе, критериями оценки. Обсуждение возможных форматов (презентация, памятка, комикс, плакат, буклет, игра).

Практика (3 ч.). Индивидуальные и групповые консультации. Выбор темы обучающимися. Сбор и систематизация материалов под руководством педагога. Работа в компьютерном классе с поисковыми системами (на проверенных сайтах) для поиска информации.

Тема 6.2. Создание итогового проекта (4ч.). *Практика (4 ч.).* Работа над проектом: создание презентации, памятки, комикса, плаката, буклета или другого продукта в выбранном формате. Использование компьютеров, графических редакторов, текстовых редакторов. Консультации педагога.

Тема 6.3. Защита итоговых проектов (4ч.). *Теория (1 ч.).* Правила публичного выступления: как представить свой проект, на что обратить внимание.

Практика (3 ч.). Презентация итоговых проектов обучающимися. Обсуждение, вопросы от других участников, обратная связь от педагога. Оценивание проектов по заранее объявленным критериям.

Тема 6.4. Заключительное занятие (2ч.). *Практика (2 ч.).* Решение проблемных кейсов. Рефлексия: «Чему я научился за год», «Что было самым важным», «Что я буду применять в жизни». Награждение самых активных обучающихся. Вручение памятных дипломов или сертификатов.

1.4. Планируемые результаты

Личностные результаты:

- сформированность основ российской гражданской идентичности, чувства гордости за свою Родину, осознание ответственности за защиту информационного пространства своей страны (цифровой патриотизм);
- развитие самостоятельности и личной ответственности за свои действия в цифровой среде, понимание последствий публикации информации и общения в сети;
- сформированность установки на безопасный и здоровый образ жизни при работе с цифровыми устройствами, соблюдение режима труда и отдыха;
- развитие этических чувств, доброжелательности и эмоционально-нравственной отзывчивости, понимание чувств других людей и нетерпимость к проявлениям кибербуллинга.

Метапредметные результаты:

- освоение способов решения проблем творческого и поискового характера в процессе создания проектов по цифровой безопасности;

- овладение логическими действиями сравнения, анализа, синтеза, обобщения, классификации при оценке информации и ситуаций в цифровой среде;

- умение устанавливать аналогии и причинно-следственные связи между поведением в сети и его последствиями;

- готовность слушать собеседника и вести диалог, излагать свое мнение и аргументировать свою точку зрения при обсуждении правил безопасного поведения;

- овладение навыками смыслового чтения текстов (сообщений, писем, постов) с целью выявления признаков опасности или мошенничества;

- овладение основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в ситуациях онлайн-риска;

- умение договариваться о распределении функций и ролей в совместной деятельности при работе над групповыми проектами.

Предметные результаты:

- понимание базовых понятий цифровой безопасности: «персональные данные», «пароль», «кибербуллинг», «фишинг», «вирус», «конфиденциальность», «сетевой этикет» и умение использовать их в речи;

- знание основных видов киберугроз, с которыми могут столкнуться младшие школьники, и способов их распознавания;

- владение правилами создания надежных паролей и безопасного хранения персональных данных;

- умение применять на практике настройки конфиденциальности в играх, приложениях и на детских образовательных платформах (под руководством взрослого и самостоятельно);

- сформированность навыков безопасного общения в мессенджерах и социальных сетях: умение отличать друга от незнакомца, избегать конфликтов, не поддаваться на провокации;

- умение распознавать признаки кибербуллинга и владение алгоритмом действий в ситуации травли в сети (не отвечать, сохранить доказательства, заблокировать, рассказать взрослому);

- владение навыками критического восприятия информации: умение отличать достоверные источники от недостоверных, распознавать фишинговые письма и подозрительные ссылки;

- знание правил цифровой гигиены: ограничение времени за экраном, выполнение физминуток, правильная организация рабочего места;

- владение основами работы с компьютером и интернетом для поиска информации при соблюдении правил безопасности.

Раздел 2. Комплекс организационно-педагогических условий

2.1. Календарный учебный график.

Календарный учебный график представлен в Приложении 1.

2.2. Условия реализации программы.

Кадровое обеспечение.

Программу может преподавать педагог дополнительного образования, отвечающий Профессиональному стандарту «Педагог дополнительного образования детей и взрослых», утвержденному приказом Министерства труда. и социальной защиты Российской Федерации от 22 сентября 2021 г. N 652н. и квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональным стандартам (ФЗ №273 ст.46, ч.1). Кадровое обеспечение программы осуществляет базовая организация – МБУ ДО ДДТ.

Материально-техническое оснащение.

Реализация программы осуществляется с использованием материально-технической базы организаций-партнеров – общеобразовательных школ, которые предоставляют компьютерные классы, оснащенные современными персональными компьютерами, мультимедийным оборудованием, лицензионным программным обеспечением, а также расходными материалами (бумага, картриджи, канцелярские принадлежности), необходимыми для проведения практических занятий, творческих мастерских и проектной деятельности. Помещения для занятий соответствуют санитарно-эпидемиологическим требованиям (СП 2.4.3648-20, СанПиН 1.2.3685-21) и обеспечивают комфортные условия для образовательного процесса.

Расстановка мебели должна быть выполнена с соблюдением нормативов: учебная мебель (столы, стулья) подобрана в соответствии с ростовозрастными особенностями обучающихся 7–10 лет.

Программа может реализовываться на базе компьютерного класса общеобразовательных учреждений. Для реализации программы требуется 12–15 персональных компьютеров (рабочие места обучающихся), каждый из которых включает системный блок, монитор с диагональю не менее 39,6 см (15,6 дюйма), клавиатуру и мышь. В качестве резервного оборудования предусмотрены 2–3 ноутбука с дополнительной клавиатурой, которые также могут использоваться педагогом.

Для печати раздаточных материалов, памяток и творческих работ необходимо многофункциональное устройство (формата А4) с функциями принтера, сканера и копира. Для демонстрации учебных материалов проектором с экраном. Для воспроизведения аудиоматериалов используются две активные акустические системы (колонки).

Программное обеспечение

На всех компьютерах установлена лицензионная операционная система. Для создания текстовых документов, презентаций и обработки информации используется лицензионный или свободно распространяемый пакет офисных

программ, включающий текстовый редактор, редактор презентаций и электронные таблицы. Для выхода в интернет используется безопасный браузер с возможностью настройки родительского контроля и системой контент-фильтрации. На всех компьютерах установлено лицензионное антивирусное программное обеспечение с регулярным обновлением баз. Для создания творческих проектов (по желанию) может использоваться программа для записи и монтажа видео.

Расходные материалы и инструменты

Для обеспечения образовательного процесса необходимы следующие расходные материалы: бумага для печати формата А4 (не менее 5 пачек, плотностью 80 г/м²), бумага цветная формата А4 (5 наборов по 8–16 цветов), картон цветной (5 наборов по 8–16 цветов), ватманы формата А1 и А2 (не менее 20 штук) для создания групповых плакатов. Для творческих работ каждому обучающемуся предоставляются фломастеры (15 комплектов по 12–24 цвета), цветные карандаши (15 комплектов по 12–24 цвета), простые карандаши (15 штук), ластики (15 штук), точилки (5–6 штук). Для изобразительной деятельности необходимы краски (гуашь и акварель) – 5–6 наборов по 12–16 цветов, кисти для рисования разных размеров (15–20 штук), стаканы-непроливайки (5–6 штук). Для работы с бумагой и картоном используются клей-карандаш (15–20 штук), клей ПВА (5–6 штук с дозатором), ножницы с закругленными концами (15 пар), линейки (15 штук длиной 15–20 см). Для создания долговечных дидактических материалов используется ламинатор и пленка для ламинирования формата А4. Для игровых моментов предусмотрены бейджи с держателями (15–20 штук). Для оформления творческих работ и портфолио необходимы папки-скоросшиватели (30 штук) и файлы (50–100 штук).

Дополнительное оборудование

При необходимости организуется беспроводное подключение через Wi-Fi роутер с поддержкой современных стандартов безопасности. В кабинете в обязательном порядке имеется укомплектованная аптечка первой помощи и два огнетушителя (углекислотных или порошковых). Для контроля времени занятия установлены настенные часы.

2.3. Методическое обеспечение

Общая методика работы

Методика работы по программе базируется на принципах доступности, наглядности, деятельностного подхода и психологической комфортности. Содержание каждого занятия адаптировано для обучающихся через использование игровых метафор, сказочных образов («Цифровой лес», «Цифровой домик») и визуализацию абстрактных понятий, что делает сложные темы (фишинг, кибербуллинг, персональные данные) понятными и близкими обучающимся. Занятия строятся по принципу «от простого к сложному» и включают обязательную смену видов деятельности каждые 10–15 минут, что соответствует особенностям непроизвольного внимания обучающихся 7–10 лет и требованиям СанПиН 1.2.3685-21. Каждое занятие включает теоретическую часть (не более 20 минут), практическую работу на компьютере (15–20 минут с

обязательной физкультминуткой и гимнастикой для глаз), игровые или творческие задания, а также рефлексию.

Основные педагогические технологии.

В программе используются следующие педагогические технологии.

Игровые технологии являются ведущими, поскольку игра остается значимым видом деятельности для обучающегося младшего школьного возраста наряду с учебой. Применяются сюжетно-ролевые игры («Агенты кибербезопасности», игры-путешествия, игры-квесты («Мой цифровой двойник»). Игровая форма позволяет моделировать реальные ситуации цифрового взаимодействия и отрабатывать алгоритмы безопасного поведения в безопасной среде.

Технология проблемного обучения реализуются через создание проблемных ситуаций и постановку познавательных задач. Обучающиеся сталкиваются с необходимостью решить конкретную проблему (например, «Что делать, если незнакомец просит прислать фото?», «Как проверить, правдивая ли новость?»), самостоятельно или в группе ищут пути решения, анализируют последствия разных вариантов поведения. Это развивает критическое мышление и способность принимать осознанные решения.

Технология проектной деятельности используется при создании итоговых и промежуточных творческих работ: памяток, плакатов, комиксов, буклетов, презентаций. Обучающиеся проходят все этапы проекта: от выбора темы и сбора информации до создания готового продукта и его публичной защиты. Проектная деятельность способствует развитию творческих способностей, коммуникативных навыков и умения работать с информацией.

Информационно-коммуникационные технологии (ИКТ) являются не только предметом изучения, но и инструментом обучения. На занятиях используются мультимедийные презентации, учебные видео и мультфильмы, работа в компьютерном классе позволяет сразу применять полученные знания на практике.

Здоровьесберегающие технологии реализуются через соблюдение санитарно-гигиенических норм (освещение, температурный режим, расстановка мебели), нормирование времени работы за компьютером (не более 20–25 минут непрерывно), обязательное проведение физкультминуток, гимнастики для глаз и динамических пауз, а также через формирование у обучающихся осознанного отношения к сохранению своего здоровья при работе с цифровыми устройствами (темы раздела «Цифровое здоровье и безопасность»).

Технология сотрудничества предполагает организацию работы в парах и малых группах, что особенно важно при разновозрастном составе обучающихся. Межвозрастное взаимодействие способствует тому, что младшие обучающиеся, наблюдая за старшими, быстрее осваивают модели безопасного поведения, а старшие, помогая младшим, закрепляют собственные знания и развивают ответственность.

Методы обучения

В программе используется широкий спектр методов обучения, классифицированных по различным основаниям:

По источнику получения знаний:

- **словесные методы:** рассказ, беседа, объяснение (используются дозированно, с опорой на наглядность и жизненный опыт детей), инструктаж перед практической работой;
- **наглядные методы:** демонстрация презентаций, учебных видео, мультфильмов, плакатов, работа с карточками, показ образцов выполнения заданий, демонстрация интерфейсов на интерактивной доске;
- **практические методы:** практические работы на компьютере, выполнение тренировочных упражнений, создание творческих проектов, решение ситуационных задач (кейсов), анализ конкретных ситуаций.

По характеру познавательной деятельности:

- **объяснительно-иллюстративные:** педагог объясняет, демонстрирует – обучающиеся воспринимают и запоминают (используется при введении нового материала).
- **репродуктивные:** выполнение заданий по образцу, отработка алгоритмов (например, алгоритма действий при кибербуллинге).
- **проблемного изложения:** педагог ставит проблему и показывает путь ее решения.
- **частично-поисковые (эвристические):** обучающиеся под руководством педагога ищут решение проблемы, участвуют в коллективном поиске.
- **исследовательские:** самостоятельное исследование ситуаций, поиск информации, анализ и обобщение (в рамках проектной деятельности).

Специфические методы, используемые в программе:

- **метод кейсов (анализ конкретных ситуаций):** обучающимся предлагаются адаптированные для их возраста ситуации (карточки с историями), которые необходимо проанализировать, определить ошибки героев и предложить правильные действия. Этот метод особенно эффективен при изучении тем «Кибербуллинг», «Фишинг», «Незнакомцы в сети».
- **игровой метод:** ролевые игры, игры-тренинги, игры-квесты, соревнования.
- **метод проектов:** самостоятельная творческая работа над созданием конкретного продукта.
- **метод рефлексии:** осмысление собственной деятельности, самооценка, обсуждение того, что узнали и чему научились, что было самым важным и интересным.

Формы организации образовательного процесса

Образовательный процесс по программе организуется в различных формах, что позволяет поддерживать интерес обучающихся и обеспечивать эффективное усвоение материала:

комбинированное учебное занятие – основная форма организации обучения. Каждое занятие имеет четкую структуру: организационный момент, актуализация

знаний, теоретическая часть, практическая работа, физкультминутка, игровое или творческое задание, рефлексия;

занятие-игра (ролевая игра, игра-путешествие, игра-квест, игра-тренинг) – используется для закрепления материала в увлекательной форме, моделирования реальных ситуаций, отработки навыков безопасного поведения;

практикум – занятие, посвященное преимущественно практической работе на компьютере (отработка навыков создания паролей, настройки конфиденциальности, поиска информации, работы с тренажерами);

творческая мастерская – занятие, на котором обучающиеся занимаются созданием творческих продуктов (памяток, плакатов, комиксов, рисунков) как индивидуально, так и в группах;

занятие-анализ – разбор конкретных ситуаций (кейсов), просмотр и обсуждение видео, работа с карточками;

занятие-проект – этапы работы над итоговым или промежуточным проектом;

занятие-презентация – защита итоговых проектов, демонстрация результатов работы;

диагностическое занятие – проведение стартовой, промежуточной и итоговой диагностики (тестирование, наблюдение, анализ творческих работ).

В программе активно используются как **фронтальные** (работа со всей группой при объяснении нового материала, демонстрации), так и **групповые** (работа в малых группах, парах при решении кейсов, создании проектов).

Методические материалы. Для успешной реализации программы разработан комплекс методических материалов:

- методические разработки всех занятий (36 конспектов) с подробным описанием хода занятия, используемых методов и приемов;
- мультимедийные презентации к занятиям;
- подборка учебных видео- и мультипликационных фильмов по темам программы;
- контрольно-измерительные материалы для проведения стартовой, промежуточной и итоговой диагностики (тесты, опросники, критерии оценки проектов).

Учет индивидуальных особенностей обучающихся.

Методика работы по программе строится с учетом индивидуальных особенностей обучающихся:

- для детей с разным темпом усвоения материала предусмотрены дифференцированные задания (более простые или более сложные варианты);
- для детей, испытывающих трудности, организуется индивидуальная помощь педагога или помощь более старших обучающихся (межвозрастное взаимодействие);
- творческие задания позволяют каждому ребенку проявить себя в соответствии со своими склонностями и способностями (кто-то лучше рисует, кто-то лучше пишет тексты, кто-то генерирует идеи);

- в программе используются задания разного уровня сложности, что позволяет поддерживать интерес как у детей с высоким уровнем подготовки, так и у начинающих.

Дидактические и игровые материалы

В процессе реализации программы используются комплекты дидактических материалов, разработанные педагогом или приобретенные в готовом виде. Это наборы карточек для игр по темам: «Безопасно — опасно», «Можно — нельзя», «Найди ловушку», «Виды киберугроз» (15–20 комплектов, желательно ламинированных). Для закрепления материала применяются настольные игры по цифровой безопасности (3–5 штук), например «Кибердром» или аналоги. Для творческих заданий необходимы наборы сюжетных картинок для составления комиксов и историй (10–15 комплектов по 10–20 картинок). В электронном и печатном виде подготовлены шаблоны памяток, плакатов, буклетов (15–20 видов). Кабинет оснащается демонстрационными плакатами по цифровой безопасности (комплект из 5–10 плакатов). Для занятий разработаны мультимедийные презентации. Имеется подборка учебных видео- и мультипликационных фильмов по цифровой безопасности (набор ссылок на проверенные образовательные ресурсы). Педагогом разработан сборник кейсов (ситуационных задач) для анализа, адаптированных для обучающихся 7–10 лет.

2.4. Формы контроля и аттестации.

Система контроля по программе «Цифровая безопасность» включает входной, текущий, промежуточный и итоговый контроль (подведение итогов реализации программы), что позволяет отслеживать динамику освоения материала и своевременно корректировать образовательный процесс.

Входной контроль проводится на первом занятии в форме **тестирования (стартовая диагностика) (сентябрь).**

Текущий контроль осуществляется на каждом занятии и направлен на оперативную проверку усвоения материала. Формы текущего контроля соответствуют специфике каждой темы и указаны в учебном плане: устный опрос**,** практическое задание**,** наблюдение**,** творческая работа**,** беседа**,** практикум по созданию паролей**, п**рактическая работа, анализ кейсов**.**

Промежуточный контроль проводится по итогам полугодия (декабрь). позволяет оценить уровень освоения завершенного блока тем. Форма промежуточного контроля: квест.

Подведение итогов реализации программы (итоговый контроль) проводится по окончании программы в мае, включает защиту итогового проекта – демонстрация творческого продукта, отражающего знания и умения по выбранной теме, решение проблемных кейсов – комплексная проверка способности применять полученные знания в смоделированных ситуациях, итоговое тестирование – оценка усвоения основных понятий и правил, диагностика личностных результатов – педагогическое наблюдение и рефлексивные методики.

2.5. Диагностический инструментарий.

Входной контроль - тестирование . (Приложение 1).

Текущий контроль осуществляется на каждом занятии и направлен на оперативную проверку усвоения материала. Формы текущего устный опрос, практическое задание, наблюдение, творческая работа (создание памяток, аватаров, комиксов, плакатов, позволяющее оценить понимание темы через продукт деятельности), беседа – обсуждение вопросов, выявление осознанности знаний, умения аргументировать, практикум по созданию паролей, практическая работа, анализ кейсов (разбор предложенных ситуаций, выявление ошибок и предложение правильных решений).

Промежуточный контроль проводится по итогам полугодия (декабрь). позволяет оценить уровень освоения завершенного блока тем. Форма промежуточного контроля: квест.

Подведение итогов реализации программы (итоговый контроль) проводится в формах защиты проекта, решение проблемных кейсов.

Средства контроля:

Входной контроль проводится на первом занятии с целью определения исходного уровня цифровой грамотности обучающихся, выявления имеющихся знаний о безопасном поведении в сети, а также индивидуальных особенностей и образовательных потребностей детей. Диагностика осуществляется в форме адаптированного тестирования «Я и Интернет» (Приложение 2), которое включает 10 заданий с визуальной поддержкой (картинки, схемы), простыми формулировками и игровыми элементами. Тест позволяет оценить знания об устройстве компьютера, базовых правилах безопасности, а также реальный цифровой опыт ребенка. Результаты фиксируются в индивидуальной карте обучающегося и используются для корректировки содержания программы с учетом выявленного уровня подготовки группы.

Текущий контроль осуществляется на каждом занятии и включает практическое задание, наблюдение, творческая работа, беседа, практикум, практическая работа на ПК, анализ кейсов, ролевая игра, анализ сайтов, устный опрос по темам программы (с оценкой по трехбалльной системе) и анализ проблемных кейсов, моделирующих реальные ситуации цифрового взаимодействия. Полный перечень вопросов, ситуационных задач и критерии оценивания представлены в Приложении 3.

Промежуточный контроль проводится для оценки уровня освоения изученного материала декабре он реализуется в форме Новогоднего квеста «Агенты кибербезопасности спешат на помощь», охватывающего темы первых двух разделов и начала третьего. Диагностические материалы (критерии оценки, карта наблюдения, бланки фиксации результатов) представлены в Приложении 4

Подведение итогов реализации программы. Подведение итогов реализации программы осуществляется в конце учебного года в форме защиты итогового проекта и решения проблемных кейсов, итогового тестирования и педагогической диагностики с применением рефлексивых методик: Анкета «Я в

цифровом мире» — самооценка обучающимися своих знаний, умений и изменений в поведении после освоения программы (10 утверждений с выбором ответа), рефлексия после защиты проекта — устное обсуждение по кругу («Что у меня получилось лучше всего?», «Что было самым трудным?», «Чему я научился, пока делал проект?»), «Лестница успеха» — графическая самооценка, на какую ступеньку обучающийся себя ставит по итогам всей программы (высокая, средняя, низкая). «Цветовые индикаторы» — выбор цвета, отражающего эмоциональное отношение к результатам своего обучения (зеленый – доволен, желтый – есть сомнения, красный – недоволен). Диагностические материалы для оценки достижения планируемых результатов представлены в Приложении 5.

Автором диагностического инструментария является разработчик программы.

2.6. Рабочая программа воспитания. Календарный план воспитательной работы.

Цель воспитательного процесса: формирование и развитие личности обучающихся на основе традиционных российских духовно-нравственных ценностей, создание условий для их самоопределения, социализации и воспитания гражданственности и патриотизма.

Задачи воспитательного процесса:

- формирование у обучающихся российской гражданской идентичности и патриотизма через осознание личной ответственности за безопасность информационного пространства своей страны (цифровой патриотизм), уважения к законам и правилам поведения в сети как части правовой культуры общества;
- воспитание ценностного отношения к личности, ее правам и свободам, развитие нетерпимости к любым формам унижения и дискриминации в цифровой среде (кибербуллингу, травле, манипуляциям), формирование готовности защищать и поддерживать тех, кто оказался в уязвимом положении;
- развитие нравственных качеств обучающихся: честности, доброжелательности, справедливости, эмпатии приобщение к традиционным российским ценностям взаимоуважения и взаимопомощи;
- формирование культуры здорового и безопасного образа жизни в условиях цифровой среды, осознанного отношения к сохранению физического и психического здоровья;
- формирование коммуникативной культуры, навыков сотрудничества и взаимопомощи в процессе коллективных проектов и игр, развитие умения работать в команде, договариваться и разрешать конфликты конструктивно.

Планируемые результаты:

- осознание ответственности за безопасность информационного пространства своей страны (цифровой патриотизм), уважение к законам и правилам поведения в сети как части правовой культуры российского общества;
- нетерпимость к любым формам кибербуллинга, травли и дискриминации в цифровой среде; готовность защищать и поддерживать тех, кто оказался в уязвимом положении; доброжелательность, честность, справедливость при общении в мессенджерах, социальных сетях и онлайн-играх;

- осознанное отношение к сохранению физического и психического здоровья при работе с цифровыми устройствами; соблюдение режима труда и отдыха, профилактика цифровой зависимости, забота о зрении и осанке;
- уважение к созидательному труду и творчеству других людей; ответственное отношение к созданию и распространению собственного цифрового контента (текстов, изображений, видео), понимание значимости интеллектуальной собственности;
- развитие критического мышления как основы противостояния деструктивному контенту, фейкам и информационным манипуляциям; устойчивая познавательная активность и интерес к безопасному освоению цифрового мира.
-сформированность навыков конструктивного общения, сотрудничества и взаимопомощи в процессе коллективных проектов и игр; умение договариваться, разрешать конфликты мирным путем, работать в команде.

Приоритетные направления воспитания:

Гражданско-патриотическое – формирование цифрового патриотизма, ответственного отношения к информационной безопасности своей страны.

Духовно-нравственное – воспитание нетерпимости к кибербуллингу, развитие эмпатии, честности и доброжелательности в цифровом общении.

Здоровьесберегающее – привитие культуры здорового образа жизни при работе с гаджетами, профилактика цифровой зависимости.

Познавательное – развитие критического мышления, умения противостоять информационным манипуляциям и фейкам.

Коммуникативное – формирование навыков конструктивного общения, сотрудничества и взаимопомощи в цифровой среде.

Творческое и трудовое – воспитание уважения к интеллектуальной собственности, ответственного создания и распространения цифрового контента.

Формы воспитательной работы. В рабочей программе воспитания по программе используются формы, адаптированные для обучающихся младшего школьного возраста и обеспечивающие достижение конкретных воспитательных результатов.

Игра-квест («Новогодний патруль цифровой безопасности») погружает детей в сюжет, где они, выполняя задания на станциях, закрепляют правила безопасного поведения в сети. Педагогический эффект – формирование навыков командного взаимодействия и ответственного отношения к цифровой безопасности через эмоциональное проживание игровой ситуации.

Творческая мастерская (мероприятия ко Дню матери, 23 февраля, 8 Марта, Дню семьи) позволяет детям создавать цифровые открытки и поздравления для близких. В процессе творчества они осваивают культуру поздравлений в мессенджерах, учатся подбирать добрые слова, что воспитывает уважение к родным и развивает эмоциональный интеллект.

Занятие-проект ко Дню Победы «Мы помним» направлен на создание виртуальной «Стены памяти». Обучающиеся под руководством педагога находят информацию о героях на проверенных сайтах и оформляют коллективный

цифровой продукт. Это воспитывает патриотизм через личное участие в сохранении истории и формирует навыки безопасного поиска информации.

Беседа с элементами игры (ко Дню Конституции) знакомит детей с их правами и обязанностями в доступной форме. Через разбор игровых ситуаций («Мои цифровые права») они усваивают правовые нормы и учатся применять их в реальной жизни.

Занятие-путешествие «Россия в цифре» combines виртуальное знакомство с достопримечательностями страны и обучение безопасному поиску информации. Это расширяет кругозор и воспитывает любовь к Родине через эмоциональное переживание.

Занятие-викторина «Россия – Родина моя» в соревновательной форме закрепляет знания о символах и истории страны, воспитывая гордость за свое Отечество и активизируя познавательный интерес.

Занятие-тренинг «Доброта в сети» через проигрывание ситуаций кибербуллинга и взаимопомощи формирует конкретные навыки эмпатичного поведения, учит поддерживать тех, кто оказался в трудной ситуации.

Комбинированное занятие с творческой работой на ПК (ко Дню народного единства и Дню защиты детей) сочетает познавательную беседу о значимых датах с созданием коллективного плаката или памятки, что обеспечивает осознанное усвоение гражданских и правовых ценностей через практическую деятельность.

Технологии воспитательного процесса. Воспитательный процесс по программе строится на основе применения комплекса педагогических технологий, обеспечивающих достижение личностных результатов обучающихся.

Игровые технологии являются ведущими и реализуются через сюжетно-ролевые игры, квесты, викторины и игры-путешествия. Они позволяют моделировать реальные жизненные ситуации, в которых Обучающиеся естественным образом осваивают социально значимые нормы поведения, учатся взаимодействовать в команде, проявлять взаимопомощь и ответственность. Эмоциональная вовлеченность в игру обеспечивает глубокое присвоение нравственных ценностей.

Технология коллективного творческого дела (КТД) применяется при создании общих продуктов – плакатов, коллажей, «Стены памяти», цифровых открыток. Совместная деятельность воспитывает ответственность за общий результат, уважение к труду других, формирует опыт сотрудничества и умение договариваться. Каждый обучающийся вносит свой вклад в общее дело, что создает ситуацию значимости и признания.

Проектная технология используется при подготовке мероприятий, приуроченных к значимым датам. Работа над проектом (сбор информации, ее осмысление, создание конечного продукта) формирует познавательную активность, ценностное отношение к истории, семье и Родине через личное участие в сохранении и трансляции значимой информации.

Технология сотрудничества реализуется через организацию работы в парах и малых группах, а также межвозрастное взаимодействие. Она развивает

коммуникативные навыки, эмпатию, умение учитывать интересы других и приходить к общему решению, что особенно важно для формирования культуры общения в цифровой среде.

Информационно-коммуникационные технологии выступают не только инструментом, но и средством воспитания. Создание цифровых открыток, презентаций, коллажей формирует цифровую культуру как часть общей культуры личности, воспитывает ответственное отношение к созданию и распространению информации.

Технология создания ситуации успеха пронизывает все мероприятия: педагог создает условия, в которых каждый обучающийся может проявить свои сильные стороны и получить признание. Это формирует позитивную самооценку, мотивацию к участию в социально значимой деятельности и развивает инициативность.

Технология рефлексии завершает каждое мероприятие: обучающиеся осмысливают свое участие, оценивают свои эмоции и поведение, делятся впечатлениями. Это развивает самосознание, способность к самоанализу и нравственной самооценке.

Здоровьесберегающие технологии обеспечивают учет возрастных особенностей: в структуру каждого мероприятия включены физкультминутки, гимнастика для глаз, беседы о здоровом образе жизни в условиях цифровой среды. Это формирует ценностное отношение к своему здоровью и профилактику цифровой зависимости.

Методы воспитательного воздействия. Воспитательный процесс строится на комплексе методов, направленных на формирование у обучающихся осознанного и ответственного поведения в цифровой среде. Беседа и разъяснение помогают детям понять смысл нравственных норм и правил безопасности, а метод примера (педагога, сверстников) создаёт наглядные образцы для подражания. Создание воспитывающих ситуаций и анализ реальных кейсов побуждают делать осознанный моральный выбор в сложных обстоятельствах. Упражнения и практические задания позволяют отработать навыки безопасного поведения до автоматизма. Игровые методы – ролевые игры, квесты, тренинги – моделируют жизненные ситуации в безопасной форме, способствуя эмоциональному проживанию и закреплению правильных моделей поведения. Поощрение и создание ситуации успеха стимулируют положительные проявления, укрепляют веру в свои силы. Метод проектов вовлекает детей в коллективную творческую деятельность, воспитывая ответственность и умение сотрудничать. Рефлексия учит осмысливать свои поступки и их последствия, развивая нравственное самосознание.

Применение интерактивных форм воспитательной работы.

Применение интерактивных форм, заложенных в календарный план воспитательной работы, превращает процесс воспитания из простой трансляции знаний в пространство активного проживания и осмысления социальных норм, где каждый обучающийся становится непосредственным участником событий. Новогодний квест «Агенты кибербезопасности спешат на помощь» через

командное приключение формирует ответственное отношение к цифровым правилам и опыт взаимовыручки. Творческие мастерские ко Дню матери, 23 февраля, 8 Марта и Дню семьи, где обучающиеся создают цифровые открытки и поздравления, развивают эмпатию, культуру выражения чувств и уважение к близким. Занятие-проект «Мы помним» ко Дню Победы вовлекает обучающихся в коллективную работу по сохранению исторической памяти, воспитывая патриотизм через личное соучастие и ответственность за общий результат. Беседа с элементами игры «Конституция и я» в доступной форме знакомит с правовыми нормами: анализируя игровые ситуации, обучающиеся учатся применять знания о правах и обязанностях в реальной жизни. Занятие-путешествие «Россия в цифре» через виртуальное знакомство с достопримечательностями страны расширяет кругозор и формирует эмоционально-ценностное отношение к Родине, а занятие-викторина «Россия – Родина моя» в соревновательной форме закрепляет знания о символах и истории, воспитывая гордость за свою страну. Занятие-тренинг «Доброта в сети» через проигрывание ситуаций кибербуллинга и взаимопомощи формирует конкретные навыки эмпатичного поведения и поддержки тех, кто оказался в трудной ситуации. Комбинированные занятия с творческой работой на ПК ко Дню народного единства и Дню защиты детей сочетают осмысление гражданских ценностей с их творческим воплощением в коллективном продукте, что обеспечивает глубокое личностное присвоение этих ценностей. Таким образом, комплексное использование интерактивных форм гарантирует, что воспитательные цели не декларируются, а проживаются детьми, превращаясь в их собственные убеждения и модели поведения.

Работа с родителями. Воспитательный процесс по программе строится в тесном взаимодействии с семьями обучающихся, что является необходимым условием формирования единых требований к безопасному поведению детей в цифровой среде и преемственности семейного и дополнительного образования. Работа с родителями направлена на повышение их компетентности в вопросах цифровой безопасности, согласование воспитательных воздействий, а также вовлечение семьи в совместную творческую и познавательную деятельность.

Основные формы работы с родителями:

- индивидуальные консультации по вопросам цифрового воспитания;
- информационные памятки и рекомендации (в том числе в родительских чатах);
- открытые занятия и мастер-классы;
- совместные детско-родительские мероприятия.

В рамках рабочей программы воспитания проводится совместный детско-родительский интерактивный квиз «Цифровая безопасность всей семьей», в ходе которого команды детей и родителей выполняют игровые задания на знание правил безопасного поведения в интернете, обсуждают реальные ситуации и совместно создают семейные памятки-подсказки по защите от цифровых угроз. Такая форма позволяет не только закрепить полученные знания, но и выстроить доверительный диалог между детьми и родителями по актуальным вопросам безопасности в сети.

Календарный план воспитательной работы

Таблица 2.

№ п/п	Название мероприятия, события	Цель	Краткое содержание	Форма проведения	Сроки проведения	Ответственные
1	«Доброта в сети: день помощи и поддержки»	Воспитание эмпатии, доброты нетерпимости к кибербуллингу, формирование навыков взаимопомощи	Беседа о доброте и взаимопомощи, разбор ситуаций, когда кто-то нуждается в поддержке в сети, создание «Добрых посланий» для одноклассников (в виде цифровых стикеров или рисунков), памятка «Как поддержать друга в сети»	Занятие-тренинг	Сентябрь	Педагог дополнительного образования
2	Совместный детско-родительский интерактивный квиз «Цифровая безопасность всей семьей»	Формирование совместных подходов к цифровой безопасности в семье, повышение родительской компетентности, закрепление знаний детей через	Команды детей и родителей выполняют игровые задания на знание правил безопасного поведения в интернете, обсуждают реальные ситуации, совместно создают семейные памятки-подсказки по защите от цифровых угроз	Интерактивный квиз, творческая мастерская	Октябрь	Педагог дополнительного образования

№ п/п	Название мероприятия, события	Цель	Краткое содержание	Форма проведения	Сроки проведения	Ответственные
		совместную деятельность				
3	«Единство в сети: урок цифрового патриотизма» (ко Дню народного единства)	Формирование гражданской идентичности, воспитание уважения к культуре и традициям разных народов, знакомство с правилами межкультурного общения в интернете	Беседа о значении единства народов России, просмотр видеоролика о дружбе и взаимопомощи, обсуждение правил уважительного общения в сети с представителями разных культур, создание коллективного плаката «Мы разные, но мы вместе» в графическом редакторе	Комбинированное занятие, творческая работа	Ноябрь	Педагог дополнительного образования
4	«Мама в цифровом мире» (ко Дню матери)	Воспитание уважения и любви к матери, развитие творческих способностей, формирование навыков безопасного общения в мессенджерах	Подготовка поздравлений для мам в текстовом редакторе, создание цифровых открыток, обсуждение правил безопасного общения в семейных чатах, конкурс «Самое тёплое пожелание маме»	Творческая мастерская	Последняя неделя ноября	Педагог дополнительного образования

№ п/п	Название мероприятия, события	Цель	Краткое содержание	Форма проведения	Сроки проведения	Ответственные
5	«Новогодний патруль цифровой безопасности»	Закрепление правил безопасного поведения в сети в игровой форме, создание праздничного настроения	Командная игра-квест по станциям: «Собери компьютер», «Цифровой домик», «Пароль для Деда Мороза», «Агент под прикрытием», «Вежливый чат». Подведение итогов первого полугодия, вручение дипломов	Игра-квест	Последняя неделя декабря	Педагог дополнительного образования
6	«Конституция и я: права и обязанности в цифре» (ко Дню Конституции)	Формирование правовой культуры, знакомство с правовыми аспектами защиты персональных данных, воспитание уважения к закону	Беседа о правах и обязанностях граждан, обсуждение права на неприкосновенность частной жизни и его применении в интернете, игра «Мои цифровые права» (распределение ситуаций на «право» и «обязанность»)	Беседа с элементами игры	Декабрь	Педагог дополнительного образования
7	«Россия в цифре: безопасное путешествие по родной стране»	Воспитание любви к Родине, развитие познавательного интереса, формирование навыков	Виртуальное путешествие по достопримечательностям России с использованием безопасных поисковых систем, создание памятки «Как искать информацию о	Занятие-путешествие	Февраль	Педагог дополнительного образования

№ п/п	Название мероприятия, события	Цель	Краткое содержание	Форма проведения	Сроки проведения	Ответственные
		безопасного поиска информации	родном крае», обсуждение фейков об истории			
8	«Подарок защитнику» (ко Дню защитника Отечества)	Воспитание уважения к защитникам Отечества, развитие творческих способностей, формирование навыков безопасного общения в мессенджерах	Создание поздравительных цифровых открыток для пап и дедушек, обсуждение правил безопасной отправки сообщений и файлов, конкурс на лучшее поздравление	Творческая мастерская	20–22 февраля	Педагог дополнительного образвания
9	«Весенний цифровой букет» (к 8 Марта)	Воспитание уважения к женщинам, девочкам, развитие творческих способностей, формирование культуры поздравлений в сети	Создание интерактивных открыток в графическом редакторе, обсуждение правил этикета при поздравлениях в мессенджерах (что писать, какие отправлять картинки), поздравление девочек группы	Творческая мастерская	Март	Педагог дополнительного образования

№ п/п	Название мероприятия, события	Цель	Краткое содержание	Форма проведения	Сроки проведения	Ответственные
10	«Мы помним: цифровая память о героях» (ко Дню Победы)	Воспитание патриотизма, уважения к истории и ветеранам, формирование навыков безопасного поиска информации о Великой Отечественной войне	Беседа о Великой Отечественной войне, знакомство с проверенными сайтами о войне (память-народа.рф), создание виртуальной «Стены памяти» (коллажа из фотографий и поздравлений)	Занятие-проект	Май	Педагог дополнительного образования
11	«Моя семья в цифре» (к Международному дню семьи)	Воспитание семейных ценностей, формирование культуры общения в семейных чатах, развитие навыков совместной творческой деятельности	Обсуждение правил общения в семейных мессенджерах, создание цифрового семейного древа или семейного фотоальбома (с согласия родителей), беседа о важности помощи старшим в освоении цифровых устройств	Творческая мастерская	Май	Педагог дополнительного образования
12	«День защиты детей в цифровом мире»	Формирование правовой грамотности, воспитание	Беседа о правах детей, обсуждение права на защиту от вредной информации, создание памятки «Мои	Комбинированное занятие	Последняя неделя мая	Педагог дополнительного образования

№ п/п	Название мероприятия, события	Цель	Краткое содержание	Форма проведения	Сроки проведения	Ответственные
		ответственного отношения к своей безопасности, знакомство с правами ребенка в цифровой среде	цифровые права и обязанности» (на бумаге или в редакторе)			

Список литературы.

Список актуальных нормативно-правовых документов.

1. Конституция РФ (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
2. Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 28.02.2025) «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 11.03.2025, далее - ФЗ №273).
3. Распоряжение Правительства РФ от 31.03.2022 г. № 678-р «Концепция развития дополнительного образования детей до 2030 года» (далее - Концепция).
4. Федеральный закон РФ от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» (с изменениями от 29.12.2022г.).
5. Указ президента РФ от 07.05.2024 г. №309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года».
6. Указ Президента РФ от 09.11.2022 №809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей».
7. Приказ Министерства просвещения РФ от 27.06.2022 г. № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»
8. Приказ Министерства просвещения РФ от 03.09.2019 № 467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей» (в редакции от 21.04.2023г.).
9. Постановление Главного государственного санитарного врача РФ от 28.09.2020 г. № 28 «Об утверждении санитарных правил СП 2.4.3648-20.
10. Постановление Главного государственного санитарного врача Российской Федерации от 28.01.2021 № 2 «Об утверждении санитарных правил и норм СанПиН 1.2.368521 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания»
11. Приказ Управления образования от 23.08.2023 № УОПР-643 «О проведении независимой оценки качества дополнительных общеобразовательных программ образовательных организаций в городе Ростове-на-Дону».
12. Приказ Министерств общего и профессионального образования Ростовской области от 01.08.2023 г. № 718 «О проведении независимой оценки качества дополнительных общеобразовательных программ в Ростовской области».
13. Приказ Управления образования от 16.11.2023 г. № УОПР-982 «Об утверждении Требований к условиям и порядку оказания муниципальной услуги в социальной сфере «Реализация дополнительных общеразвивающих программ (общественной экспертизы) на соответствие Требованиям к условиям и порядку оказания муниципальной услуги

«реализация дополнительных общеразвивающих программ» в соответствии с социальными сертификатами.

14. Приказ Минобразования РО №136 от 14.02.2024г. «О внесении изменений в приказ минобразования Ростовской области от 01.08.2023 № 718».

15. Приказ Минобразования РО №724 от 03.08.2023г. «Об утверждении Требований к условиям и порядку оказания государственной услуги в социальной сфере „Реализация дополнительных общеразвивающих программ“ в Ростовской области».

16. Письмо Министерства Просвещения Российской Федерации № АБ-3936/06 от 29.09.2023 «Методические рекомендации по формированию механизмов обновления содержания, методов и технологий обучения в системе дополнительного образования детей»

17. Письмо Министерства образования и науки РФ от 18 ноября 2015 г. № 09-3242 «О направлении информации» (вместе с «Методическими рекомендациями по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы)»)

18. Приказ Министерства общего и профессионального образования Ростовской области от 03.08.2023 года № 724 «Об утверждении Требований к условиям и порядку оказания государственной услуги в социальной сфере «Реализация дополнительных общеразвивающих программ»».

19. Приказ Управления образования города Ростова-на-Дону от 21 февраля 2024 года №УОПР/158 «О внесении изменений в приказ Управления образования города Ростова-на-Дону от 15 декабря 2023 года №УОПР/1100».

20. Методические рекомендации по оформлению структурных элементов дополнительных общеразвивающих программ, утвержденные на заседании методического совета ГАУ ДПО РО «Институт развития образования», протокол от 29.03.2024 г. № 3.

21. Письмо Минобразования РО ГАУ ДПО РО ИРО от 09.04.2024 Рекомендации по оформлению и содержанию структурных элементов, Пр. от 29.03.2024 г.№3.

Список литературы для педагогов.

1. Богданов, С. А. Методика использования цифровых технологий для обеспечения информационной безопасности учащихся / С. А. Богданов, С. В. Алексеев, Т. А. Спицына, М. Е. Успенская // Российский государственный педагогический университет им. А. И. Герцена. – 2025. – С. 45–52.

2. Нагаева, Л. Г. Кибербезопасность для детей и родителей / Л. Г. Нагаева. – Ростов-на-Дону : Феникс, 2022. – 156 с.

3. Пазухина, С. В. Превентивные технологии защиты детей от вредной информации : учебное пособие для педагогов / С. В. Пазухина, С. А. Филиппова. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2026. – 194 с. – (Профессиональное образование).

4. Риски в цифровой среде: диагностика, профилактика, коррекция : учебно-методическое пособие для учителей общеобразовательных учреждений / под

ред. Е. В. Шпагиной ; Альянс по защите детей в цифровой среде. – Москва, 2024. – 168 с.
5. Толстых, О. С. Цифровые технологии как средство визуализации при обучении безопасному поведению младших школьников / О. С. Толстых, Н. А. Амбарцумян, Е. Г. Костенко // Бизнес. Образование. Право. – 2025. – № 2 (71). – С. 473–479.
6. Цифровые технологии в современном дошкольном образовании : монография / Ю. А. Дмитриев, О. Л. Зверева, Т. В. Калинина [и др.] ; отв. ред. О. Л. Зверева ; Московский педагогический государственный университет. – Москва : МПГУ, 2024. – 223 с.
7. Шаркова, Е. А. Азбука цифровой безопасности / Е. А. Шаркова. – Санкт-Петербург : Питер, 2023. – 64 с.
8. Якунина, Т. В. Безопасность в интернете : детская энциклопедия / под ред. Т. В. Якуниной. – Москва : Росмэн, 2023. – 96 с.

Список литературы для обучающихся.

1. Богданов, С. А. Методика использования цифровых технологий для обеспечения информационной безопасности учащихся / С. А. Богданов, С. В. Алексеев, Т. А. Спицына, М. Е. Успенская // Российский государственный педагогический университет им. А. И. Герцена. – 2025. – С. 45–52.
2. Нагаева, Л. Г. Кибербезопасность для детей и родителей / Л. Г. Нагаева. – Ростов-на-Дону : Феникс, 2022. – 156 с.
3. Пазухина, С. В. Превентивные технологии защиты детей от вредной информации : учебное пособие для педагогов / С. В. Пазухина, С. А. Филиппова. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2026. – 194 с. – (Профессиональное образование).
4. Толстых, О. С. Цифровые технологии как средство визуализации при обучении безопасному поведению младших школьников / О. С. Толстых, Н. А. Амбарцумян, Е. Г. Костенко // Бизнес. Образование. Право. – 2025. – № 2 (71). – С. 473–479.
5. Цифровые технологии в современном дошкольном образовании: монография / Ю. А. Дмитриев, О. Л. Зверева, Т. В. Калинина [и др.]; отв. ред. О. Л. Зверева ; Московский педагогический государственный университет. – Москва : МПГУ, 2024. – 223 с.
6. Шаркова, Е. А. Азбука цифровой безопасности / Е. А. Шаркова. – Санкт-Петербург : Питер, 2023. – 64 с.
7. Якунина, Т. В. Безопасность в интернете : детская энциклопедия / под ред. Т. В. Якуниной. – Москва : Росмэн, 2023. – 96 с.

Список Интернет-ресурсов.

1. Материалы «Лаборатории Касперского» по цифровой безопасности в библиотеке Московской электронной школы (МЭШ) school.mos.ru
2. Серия книг «Лаборатории Касперского»: «Мидори Кума и необычная гонка», «Сказки о цифровой безопасности» kids.kaspersky.ru

3. Формирование позиции в деструктивном информационном поле: методические рекомендации для педагогов / проект «Как пережить информационные войны https://nro.center/infowars/
4. Серия книг «Лаборатории Касперского»: «Мидори Кума и необычная гонка», «Сказки о цифровой безопасности» kids.kaspersky.ru
5. Уроки цифровой грамотности на платформе «Учи.ру» [Электронный ресурс]. uchi.ru
6. Детский портал «Спас-Экстрим» : правила безопасности в интернете [Электронный ресурс]. spasextreme.mchs.ru

2.7. Приложения

Приложение 1. Календарный учебный график

Календарный учебный график

Таблица 3.

№ п/п	Дата	Тема занятия	Кол-во часов	Время проведения	Форма занятия	Место проведения	Форма контроля
Раздел 1. Введение в цифровую безопасность (10 часов)							
1		Вводное занятие. Инструктаж по технике безопасности. Стартовая педагогическая диагностика	2		беседа с элементами игры	МБОУ «Школа №83»	тестирование (входная диагностика)
2		Что такое Интернет: возможности и опасности	2		занятие-путешествие	МБОУ «Школа №83»	устный опрос
3		Компьютер и устройство: правила безопасного использования	2		комбинированное занятие	МБОУ «Школа №83»	практическое задание
4		Мои цифровые помощники (браузеры, поисковики, приложения)	2		практикум	МБОУ «Школа №83»	наблюдение
5		Создание памятки «Правила безопасного старта»	2		творческая мастерская	МБОУ «Школа №83»	творческая работа
Раздел 2. Персональные данные и цифровой профиль (12 часов)							
6		Что такое персональные	2		занятие-сказка	МБОУ «Школа №83»	беседа

№ п/п	Дата	Тема занятия	Кол-во часов	Время проведения	Форма занятия	Место проведения	Форма контроля
		данные? Личное и публичное					
7		Пароли: секреты надежной защиты	2		практикум-игра	МБОУ «Школа №83»	практикум по созданию паролей
8		Аватар, никнейм и профиль: безопасное представление себя в сети	2		творческая мастерская	МБОУ «Школа №83»	творческое задание
9		Настройки конфиденциальности в играх и приложениях	2		практикум	МБОУ «Школа №83»	практическая работа на ПК
10		Что нельзя публиковать в соцсетях? Разбор ситуаций	2		занятие-анализ	МБОУ «Школа №83»	анализ кейсов
11		Квест «Мой цифровой двойник»	2		игра-квест	МБОУ «Школа №83»	
Раздел 3. Безопасное общение в цифровой среде (14 часов)							
12		Правила этикета в мессенджерах и соцсетях	2		ролевая игра	МБОУ «Школа №83»	ролевая игра
13		Друзья и незнакомцы в сети: как отличить и не ошибиться	2		занятие-рассуждение	МБОУ «Школа №83»	анализ ситуаций
14		Что такое кибербуллинг? Как распознать и что делать	2		беседа с элементами тренинга	МБОУ «Школа №83»	беседа, тренинг

№ п/п	Дата	Тема занятия	Кол-во часов	Время проведения	Форма занятия	Место проведения	Форма контроля
15		Если обижают в сети: алгоритмы помощи и поддержки	2		ролевая игра-тренинг	МБОУ «Школа №83»	ролевая игра
16		Добрые и злые сообщения: учимся различать намерения	2		практикум с элементами игры	МБОУ «Школа №83»	практикум
17		Создание комикса «История одной переписки» Тренинг «Безопасный чат»	2		творческая мастерская	МБОУ «Школа №83»	творческий проект
18		Новогодний квест «Агенты кибербезопасности спешат на помощь»	2		игра-тренинг	МБОУ «Школа №83»	Анализ квеста
Раздел 4. Информационная безопасность: учимся думать критически (12 часов)							
19		Правда и ложь в Интернете: как проверить информацию	2		практикум - исследование	МБОУ «Школа №83»	практикум с поисковиками
20		Фишинг: опасные ссылки и подозрительные письма	2		занятие-тренинг	МБОУ «Школа №83»	тренинг на тренажере
21		Вирусы и вредоносные программы: что это и как защититься	2		комбинированное занятие	МБОУ «Школа №83»	практическая работа
22		Реклама и ловушки: учимся говорить «нет»	2		анализ сайтов	МБОУ «Школа №83»	анализ сайтов

№ п/п	Дата	Тема занятия	Кол-во часов	Время проведения	Форма занятия	Место проведения	Форма контроля
23		Создание памятки «Проверяй, прежде чем нажать»	2		творческая мастерская	МБОУ «Школа №83»	творческая работа
24		Итоговое занятие по модулю: игра-соревнование «Детективы информации»	2		командная игра	МБОУ «Школа №83»	командная игра
Раздел 5. Цифровое здоровье и безопасность (10 часов)							
25		Время за компьютером: сколько можно и как не навредить себе	2		беседа с элементами практикума	МБОУ «Школа №83»	беседа, составление режима
26		Осанка, зрение и физминутки: заботимся о здоровье	2		занятие-практикум	МБОУ «Школа №83»	практикум (физминутки)
27		Игры: полезные, бесполезные и опасные	2		анализ игр	МБОУ «Школа №83»	анализ игр
28		Как не попасть в зависимость от гаджетов	2		занятие-тренинг	МБОУ «Школа №83»	тренинг
29		Создание плаката «Здоровый цифровой образ жизни»	2		творческая мастерская	МБОУ «Школа №83»	творческая работа
Раздел 6. Итоговая аттестация и проектная деятельность (14 час)							
30		Подготовка итогового проекта (выбор темы, сбор материалов)	2		занятие-консультация	МБОУ «Школа №83»	консультация

№ п/п	Дата	Тема занятия	Кол-во часов	Время проведения	Форма занятия	Место проведения	Форма контроля
31		Подготовка итогового проекта (работа с информацией)	2		практикум	МБОУ «Школа №83»	наблюдение
32		Создание итогового проекта (работа над продуктом)	2		творческая мастерская	МБОУ «Школа №83»	самостоятельная работа
33		Создание итогового проекта (оформление)	2		творческая мастерская	МБОУ «Школа №83»	самостоятельная работа
34		Защита итоговых проектов	2		презентация проектов	МБОУ «Школа №83»	презентация проекта
35		Защита итоговых проектов	2		презентация проектов	МБОУ «Школа №83»	презентация проекта
36		Заключительное занятие	2		итоговое занятие	МБОУ «Школа №83»	комплексное тестирование, рефлексия
		Итого	**72**				

Приложение 2. Диагностические материалы для входного контроля.

Входной контроль (стартовая диагностика)

Для определения исходного уровня цифровой грамотности обучающихся 7–10 лет на первом занятии проводится тестирование «Я и Интернет». Тест адаптирован для младших школьников: содержит 10 заданий с визуальной поддержкой (картинки, схемы), простые формулировки и игровые элементы. Задания направлены на выявление имеющихся знаний об устройстве компьютера, базовых правилах безопасного поведения в сети, а также на оценку цифрового опыта ребенка.

Таблица 4

Структура теста

№	Задание	Форма	Проверяемая область
1	**«Собери картинку»** – соедини название устройства (монитор, клавиатура, мышь, системный блок) с его изображением	Соедини линиями	Знание основных устройств компьютера
2	**«Для чего это нужно?»** – выбери правильное назначение для каждого устройства (например, принтер – печатает, наушники – слушать)	Выбор из 2–3 вариантов	Понимание функций устройств
3	**«Что такое Интернет?»** – выбери правильный ответ: а) игра, б) сеть, соединяющая компьютеры, в) программа	Один правильный ответ	Представление об Интернете
4	**«Можно – нельзя»** – отметь знаком ✓, что можно делать в Интернете: играть в обучающие игры, смотреть мультфильмы, открывать письма от незнакомцев, общаться с родителями	Отметка в таблице	Первичное понимание безопасного поведения
5	**«Опасный незнакомец»** – рассмотри картинку (ребенок общается в чате с незнакомцем). Что нужно сделать? а) продолжить общаться, б) рассказать родителям, в) дать свой номер телефона	Выбор ответа	Реакция на контакт с незнакомцем
6	**«Секретный пароль»** – какой пароль надежнее: а) 12345, б) qwerty, в) R2d2!9? (объясни, почему)	Выбор и объяснение	Понимание важности сложных паролей

№	Задание	Форма	Проверяемая область
7	**«Личное или общее»** – распредели слова (имя, фамилия, адрес, любимый цвет, номер школы, кличка собаки) в две колонки: можно сказать всем / только семье	Распределение	Различение персональных данных
8	**«Вредный вирус»** – что делать, чтобы компьютер не заболел? а) установить антивирус, б) играть целый день, в) скачивать всё подряд	Выбор ответа	Базовые представления о защите
9	**«Здоровье за компьютером»** – отметь правильную позу за компьютером (на картинке три варианта: сутулый, слишком близко, ровно)	Выбор картинки	Знание правил здоровьесбережения
10	**«Мой цифровой день»** – закрась кружочки: сколько часов в день ты обычно проводишь за компьютером/планшетом? (0–1 час, 1–2 часа, больше 2 часов)	Графический выбор	Оценка реальной цифровой нагрузки

Проведение: тест занимает 20–25 минут, проводится в спокойной доброжелательной обстановке. Результаты фиксируются в индивидуальной карте обучающегося и позволяют педагогу выявить «зоны риска», адаптировать программу под уровень группы и отследить динамику в конце года.

Приложение 3. Диагностические материалы для текущего контроля

Диагностические материалы для текущего контроля

I. УСТНЫЙ ОПРОС

Устный опрос проводится на различных этапах занятия (актуализация знаний, закрепление, рефлексия) и позволяет быстро оценить уровень понимания материала. Вопросы группируются по темам программы. Оценка ответов производится по трехбалльной системе (см. критерии в конце раздела).

Тема 1.2. Что такое Интернет: возможности и опасности

Вопросы к устному опросу

Таблица 5

№	Вопрос	Правильный ответ (ориентир)
	Что такое Интернет?	Это сеть, которая соединяет компьютеры по всему миру, помогает учиться, общаться, играть
2	Какие полезные вещи можно делать в Интернете?	Учиться, смотреть обучающие видео, общаться с друзьями, играть в развивающие игры
3	Какие опасности могут встретиться в Интернете?	Мошенники, вирусы, незнакомцы, которые могут обидеть или обмануть
4	Кого называют «цифровым хищником»?	Человека, который притворяется другом, чтобы обмануть или обидеть
5	Что делать, если ты встретил в Интернете что-то страшное или непонятное?	Рассказать родителям или учителю

Тема 2.1. Что такое персональные данные? Личное и публичное

Таблица 6.

№	Вопрос	Правильный ответ (ориентир)
1	Что такое персональные данные?	Это информация о человеке, которая помогает его узнать (имя, фамилия, адрес, фото)

№	Вопрос	Правильный ответ (ориентир)
2	Почему нельзя публиковать свой адрес в Интернете?	Чтобы незнакомые люди не узнали, где ты живешь, и не смогли прийти
3	Какие данные можно рассказывать о себе в сети?	Имя (не полное), любимый цвет, любимую книгу, увлечения
4	Какие данные нужно всегда держать в секрете?	Фамилию, адрес, номер телефона, пароли, номер школы
5	Что такое «цифровой домик» и где в нем «сейф»?	Цифровой домик – это твоя страница в Интернете, а сейф – это личная информация, которую нельзя показывать всем

Тема 3.1. Правила этикета в мессенджерах и соцсетях

Таблица 7

№	Вопрос	Правильный ответ (ориентир)
1	Почему нельзя писать сообщения ЗАГЛАВНЫМИ БУКВАМИ?	В Интернете это считается криком, это невежливо
2	Что нужно сделать, прежде чем отправить сообщение?	Проверить, не обидит ли оно того, кто его получит
3	Можно ли отправлять много смайлов подряд?	Лучше использовать смайлы к месту, чтобы не затруднять чтение
4	Как попросить помощи в чате, если что-то непонятно?	Вежливо написать: «Извините, не могли бы вы помочь мне...»
5	Что делать, если кто-то написал тебе грубость?	Не отвечать грубостью, можно не отвечать вообще, рассказать взрослому

Тема 3.3. Что такое кибербуллинг? Как распознать и что делать

Таблица 8

№	Вопрос	Правильный ответ (ориентир)
1	Что такое кибербуллинг?	Это травля в Интернете, когда кого-то специально обижают, оскорбляют, дразнят

№	Вопрос	Правильный ответ (ориентир)
2	Какие бывают виды кибербуллинга?	Злые комментарии, исключение из игры, распространение слухов, угрозы
3	Как чувствует себя человек, которого травят в сети?	Ему грустно, обидно, страшно, он может плакать
4	Что делать, если ты стал жертвой кибербуллинга?	1) Не отвечать обидчику, 2) сделать скриншот, 3) заблокировать, 4) рассказать взрослому
5	Что делать, если ты увидел, что травят другого?	Не молчать, поддержать того, кого обижают, рассказать взрослому

Тема 4.1. Правда и ложь в Интернете: как проверить информацию

Таблица 9

№	Вопрос	Правильный ответ (ориентир)
1	Почему не всему, что написано в Интернете, можно верить?	Потому что люди могут ошибаться или специально обманывать
2	Как проверить, правдивая ли новость?	Посмотреть в другом источнике, спросить у взрослого, найти подтверждение на проверенных сайтах
3	Что такое «фейк»?	Это ложная, выдуманная информация
4	Какие новости чаще всего оказываются ложными?	Очень страшные или наоборот, очень радостные («Вы выиграли миллион!»)
5	Кому можно доверять в Интернете?	Известным детским сайтам, образовательным порталам, сайтам, которые посоветовали родители

Тема 5.1. Время за компьютером: сколько можно и как не навредить себе

№	Вопрос	Правильный ответ (ориентир)
1	Сколько времени можно проводить за компьютером ребенку 7–10 лет?	Не больше 30–40 минут в день (если не уроки)

№	Вопрос	Правильный ответ (ориентир)
2	Почему нельзя играть в компьютер долго?	Устают глаза, болит спина, не хватает времени на прогулки и живое общение
3	Какие признаки говорят о том, что пора отдохнуть?	Глаза краснеют, начинает болеть голова, хочется тереть глаза
4	Что нужно делать, чтобы сохранить здоровье за компьютером?	Сидеть ровно, делать перерывы, выполнять гимнастику для глаз
5	Какие занятия, кроме компьютера, полезны для здоровья?	Прогулки, спорт, рисование, чтение, игры с друзьями

Критерии оценки устных ответов

Таблица 10.

Уровень	Характеристика ответа
Высокий (3 балла)	Ответ полный, правильный, осознанный. Обучающийся не только называет правило, но и может объяснить, почему нужно действовать именно так, приводит примеры.
Средний (2 балла)	Ответ правильный, но неполный. Обучающийся называет правило, но затрудняется с объяснением или примерами. Может ответить с помощью наводящих вопросов.
Низкий (1 балл)	Ответ неправильный или обучающийся не может ответить даже с помощью педагога, не понимает сути вопроса.

II. АНАЛИЗ КЕЙСОВ (СИТУАЦИОННЫХ ЗАДАЧ)

Анализ кейсов проводится на занятиях, предусмотренных учебным планом (темы 2.5, 3.2, 3.5, 4.2, 4.4), а также может использоваться как элемент итоговой диагностики. Обучающимся предлагаются адаптированные для их возраста ситуации, которые необходимо проанализировать, определить ошибки героев и предложить правильные действия. Задания могут выполняться индивидуально, в парах или малых группах с последующим обсуждением.

Кейс 1. «Новый друг» (темы 2.5, 3.2)

Ситуация: «Пятиклассница Маша играла в онлайн-игру. К ней в чат написал незнакомый мальчик, представился Мишей, сказал, что ему тоже 10 лет, и предложил дружить. Они стали общаться каждый день. Через неделю Миша

попросил Машу прислать свою фотографию и сказать, в какой школе она учится, чтобы вместе ходить в кино. Маша очень обрадовалась новому другу и хотела сразу же отправить фото».

Вопросы для анализа:

1. Правильно ли поступила Маша, согласившись общаться с незнакомцем?
2. Какие опасности могут быть в такой ситуации?
3. Что нужно было сделать Маше, когда к ней обратился незнакомец?
4. Что теперь делать Маше? Посоветуйте ей правильные действия.
5. Почему нельзя отправлять незнакомцам свои фотографии и рассказывать, где ты учишься?

Правильные варианты ответов:

- Общаться с незнакомцами в сети можно только с разрешения родителей.
- Нельзя верить незнакомцу, даже если он называет себя ровесником.
- Нельзя отправлять фото и личные данные незнакомым людям.
- Правильные действия: прекратить общение, не отвечать на просьбы, рассказать родителям, заблокировать незнакомца.
- Фотографии и личные данные могут использовать мошенники.

Кейс 2. «Секрет пароля» (темы 2.2, 2.5)

Ситуация: «Петя и Коля – лучшие друзья. Однажды Петя сказал Коле: "Давай обменяемся паролями от своих страничек в игре, чтобы мы могли заходить друг к другу в гости и играть за персонажей друга. Это же весело!" Коля подумал и согласился, ведь они лучшие друзья и доверяют друг другу».

Вопросы для анализа:

1. Правильно ли поступили мальчики?
2. Почему нельзя никому сообщать свои пароли, даже лучшим друзьям?
3. Что может случиться, если пароль узнает кто-то другой?
4. Как бы вы объяснили Пете и Коле, почему так делать нельзя?
5. Какое правило создания и хранения паролей они нарушили?

Правильные варианты ответов:

- Мальчики поступили неправильно.
- Пароль – это личный секрет. Даже друг может случайно или специально сделать что-то от твоего имени.
- Если пароль узнает другой человек, он может удалить твои достижения, написать от твоего имени грубости, потратить игровую валюту.
- Пароль нельзя сообщать никому, кроме родителей (и то только в случае необходимости).
- Правило: пароль должен быть известен только тебе.

Кейс 3. «Злой комментарий» (темы 3.3, 3.4)

Ситуация: «Аня выложила в детской социальной сети свой рисунок. Она очень старалась и гордилась своей работой. Вдруг в комментариях появилось сообщение: "Фу, какая ерунда! Даже маленький ребенок нарисует лучше. Ты бездарность!" Аня расстроилась и заплакала. Ей стало обидно, и она не знала, что делать».

Вопросы для анализа:

1. Как называется такое поведение в Интернете?
2. Что чувствует Аня? Почему ей так больно?
3. Что бы вы посоветовали Ане? Как ей правильно поступить?
4. Нужно ли отвечать обидчику? Почему?
5. Кому можно рассказать о случившемся?

Правильные варианты ответов:

- Это кибербуллинг (травля в сети).
- Ане обидно, больно, она чувствует, что ее труд не оценили, ей грустно.
- Не отвечать обидчику, не вступать в перепалку, сделать скриншот комментария, заблокировать обидчика, рассказать родителям или учителю.
- Отвечать не нужно, потому что обидчик только этого и ждет (он хочет продолжения).
- Рассказать родителям, учителю, можно пожаловаться администрации сайта.

Кейс 4. «Выигрыш» (темы 4.2, 4.4)

Ситуация: «На электронную почту папы пришло письмо: "Поздравляем! Вы выиграли новый телефон! Перейдите по ссылке и введите свои данные, чтобы получить приз". Саша увидел это письмо, когда делал уроки за папиным компьютером. Он очень обрадовался и хотел скорее нажать на ссылку, чтобы помочь папе получить подарок».

Вопросы для анализа:

1. Что такое фишинг?
2. Почему письмо о выигрыше может быть опасным?
3. Что произойдет, если перейти по ссылке и ввести свои данные?
4. Как нужно поступить Саше?
5. Какие признаки выдают мошенников в этом письме?

Правильные варианты ответов:

- Фишинг – это выуживание личных данных мошенниками.
- Письма о выигрыше часто рассылают мошенники, чтобы украсть данные или заманить на опасный сайт.
- Если перейти по ссылке, можно потерять деньги или данные, компьютер может заразиться вирусом.
- Саша не должен нажимать на ссылку, нужно рассказать о письме папе и спросить его совета.
- Признаки мошенничества: неожиданный выигрыш (никто не участвовал), просьба перейти по ссылке и ввести данные, нет имени (просто «вы»).

Кейс 5. «Игра затянула» (темы 5.1, 5.4)

Ситуация: «Дима очень любит одну компьютерную игру. В выходной день он сел играть утром, а когда посмотрел на часы, оказалось, что прошло уже 4 часа. Мама звала обедать, но Дима крикнул "Сейчас!" и продолжил играть. Глаза устали, голова немного болит, но Диме очень хочется пройти сложный уровень».

Вопросы для анализа:

1. Правильно ли поступает Дима?
2. Чем опасно долгое сидение за компьютером?
3. Что такое «цифровая зависимость» и есть ли она у Димы?
4. Что нужно делать, чтобы не попасть в такую ситуацию?
5. Составьте для Димы памятку «Как не заиграться».

Правильные варианты ответов:

- Дима поступает неправильно, он вредит своему здоровью.
- Опасно: устают глаза, портится осанка, болит голова, не хватает времени на другие дела.
- У Димы начинается игровая зависимость (он не может остановиться).
- Нужно ставить таймер, договариваться с родителями о времени, делать перерывы, чередовать игру с другими занятиями.
- Памятка: 1) Ставь таймер на 30 минут, 2) Когда таймер звенит – встань и сделай зарядку, 3) Не играй больше часа подряд, 4) Сначала сделай уроки, потом играй, 5) Играй только в те игры, которые разрешили родители.

Кейс 6. «Чужой аккаунт» (темы 2.4, 3.2)

Ситуация: «Одноклассник попросил у Лены телефон, чтобы позвонить маме. Лена дала. А он зашел в ее аккаунт в соцсети и написал от ее имени глупые сообщения всем друзьям. Лена очень расстроилась и не знала, что теперь делать».

Вопросы для анализа:

1. Какое правило безопасности нарушила Лена?
2. Почему нельзя давать свой телефон другим людям (даже знакомым)?
3. Что нужно сделать Лене сейчас?
4. Как можно было избежать этой ситуации?
5. Как поступить с одноклассником?

Правильные варианты ответов:

- Лена нарушила правило: нельзя давать свой телефон другим людям без присмотра, даже знакомым.
- В телефоне могут быть личные данные, переписка, доступ к аккаунтам.
- Сейчас нужно: зайти в аккаунт, сменить пароль, проверить, что написал одноклассник, объяснить друзьям, что это не она, рассказать родителям и учителю.
- Избежать: блокировка экрана паролем, не давать телефон в руки, проследить, чтобы звонили только по делу.
- С одноклассником нужно серьезно поговорить, объяснить, что это обидно и недопустимо, рассказать взрослым.

Кейс 7. «Вирус» (тема 4.3)

Ситуация: «В игре выскочило окошко: "Ваш компьютер заражен! Срочно скачайте программу для лечения!" и большая красная кнопка "Скачать". Миша испугался и хотел нажать на кнопку, чтобы спасти компьютер».

Вопросы для анализа:

1. Что это за окошко? Правда ли компьютер заражен?
2. Что будет, если нажать на кнопку «Скачать»?

3. Как нужно поступить Мише?
4. Как защитить компьютер от настоящих вирусов?
5. Что такое антивирус и зачем он нужен?

Правильные варианты ответов:

- Это обман (фишинговая реклама), компьютер, скорее всего, не заражен. Мошенники пугают, чтобы заставить скачать вредоносную программу.
- Если нажать на кнопку, можно скачать настоящий вирус или программу-шпион.
- Мише нужно закрыть окно (нажать крестик, но не на кнопки внутри окна!), показать это окно родителям, проверить компьютер антивирусом.
- Установить антивирус, не скачивать игры с подозрительных сайтов, не нажимать на всплывающие окна.
- Антивирус – это программа-защитник, которая не пускает вирусы в компьютер и лечит его, если вирус попал.

Кейс 8. «Спор в чате» (темы 3.1, 3.5)

Ситуация: «В классном чате обучающиеся обсуждали проект. Вдруг один мальчик написал, что идея другого ребенка – глупая. Начался спор, обучающиеся стали писать резкие сообщения, обзываться. Чат превратился в перепалку».

Вопросы для анализа:

1. Какие правила общения нарушили обучающиеся?
2. Что такое троллинг? Было ли здесь это?
3. Как нужно было поступить, чтобы спор не перерос в ссору?
4. Что делать, если ты видишь, что кто-то нарушает правила?
5. Как теперь помирить участников спора?

Правильные варианты ответов:

- Нарушили правила уважения: нельзя называть чужие идеи глупыми, нельзя обзываться, нельзя писать резко.
- Троллинг – это провокация, чтобы вызвать ссору. Возможно, мальчик специально написал резко, чтобы его «зацепили».
- Нужно было сказать: «Мне кажется, идея интересная, но можно ее доработать», или промолчать, или написать в личном сообщении, что замечание было обидным.
- Если видишь нарушение, можно напомнить о правилах, поддержать того, кого обижают, позвать взрослого.
- Помирить: попросить прощения друг у друга, объяснить, что не хотели обидеть, договориться впредь обсуждать идеи, а не людей.

Критерии оценки анализа кейсов

Таблица 10

Уровень	Характеристика
Высокий (3 балла)	Обучающийся правильно определяет проблему, видит все ошибки героев, предлагает полный и правильный алгоритм действий,

Уровень	Характеристика
	аргументирует свою позицию, может привести примеры из жизни или других ситуаций.
Средний (2 балла)	Обучающийся в целом понимает ситуацию, определяет основные ошибки, предлагает правильные, но неполные действия (может упустить один из шагов), затрудняется с аргументацией.
Низкий (1 балл)	Обучающийся не понимает сути ситуации, не видит ошибок или видит не те, предлагает опасные или неэффективные действия, не может объяснить свой выбор.

Организация проведения анализа кейсов

1. Кейсы предъявляются на карточках (с иллюстрациями) или на экране (презентация).
2. Время на обсуждение: 5–7 минут для индивидуальной работы, 10–12 минут для групповой.
3. Возможно использование приема «займи позицию» – обучающиеся поднимают карточки (согласен/не согласен) или расходятся по углам класса в зависимости от выбранного решения.
4. После обсуждения обязательно проводится коллективное обсуждение правильных вариантов.
5. Результаты фиксируются в карте наблюдения или в индивидуальном листе обучающегося.

Приложение 4. Диагностические материалы для промежуточного контроля

Диагностические материалы для промежуточного контроля (декабрь)

С учетом того, что программа реализуется с сентября по май, к декабрю обучающиеся осваивают следующие разделы: Раздел 1 «Введение в цифровую безопасность» (темы: устройство компьютера, цифровые помощники, правила безопасного старта), Раздел 2 «Персональные данные и цифровой профиль» (темы: персональные данные, пароли, аватар и никнейм, настройки конфиденциальности, что нельзя публиковать) и начало Раздела 3 «Безопасное общение в цифровой среде» (темы: правила этикета, друзья и незнакомцы в сети). Для промежуточного контроля в декабре выбрана единая игровая форма, охватывающая все пройденные темы.

Форма промежуточного контроля:

Новогодний квест «Агенты кибербезопасности спешат на помощь»

Цель: комплексная проверка знаний и умений по темам, изученным в сентябре – декабре (устройство компьютера, персональные данные, пароли, аватар, настройки конфиденциальности, правила общения, распознавание незнакомцев).

Время проведения: последнее занятие перед зимними каникулами (декабрь).

Длительность: 2 часа.

Организация: обучающиеся делятся на 3–4 команды по 3–4 человека. Каждая команда получает маршрутный лист с заданиями от «штаба кибербезопасности», который нужно выполнить, чтобы помочь сказочным героям, попавшим в беду в цифровом мире. Задания расположены на пяти «станциях» (в разных зонах компьютерного класса или кабинета). На каждой станции команда выполняет задание и получает фрагмент кода, из которого в конце складывается пароль для спасения «Новогоднего огонька».

Содержание заданий:

- **Станция 1 «Собери компьютер» (тема 1.3):** из набора карточек с изображениями устройств (системный блок, монитор, клавиатура, мышь, принтер, колонки, наушники) нужно отобрать только базовые устройства компьютера и правильно назвать их функции.
- **Станция 2 «Цифровой домик» (темы 2.1, 2.5):** на плакате изображен домик с окошками. На карточках написаны виды информации: имя, фамилия, адрес, номер телефона, любимый цвет, кличка собаки, номер школы, фотография. Нужно распределить, что можно разместить на «заборе» (доступно всем), а что спрятать в «сейф» (только для себя и близких).
- **Станция 3 «Пароль для Деда Мороза» (тема 2.2):** команда получает задание придумать надежный пароль для сказочного героя (например, Снегурочки). Пароль должен соответствовать правилам: не менее 8 символов, буквы разного регистра, цифры, не использовать имя героя. Команда записывает пароль и объясняет, почему он надежный.

- **Станция 4 «Агент под прикрытием» (темы 3.2, 3.3):** команда получает карточку с описанием ситуации: «В игре написал незнакомец, представился ровесником, предлагает дружить и просит прислать фото и номер телефона». Нужно выбрать из предложенных вариантов правильные действия (например: заблокировать и рассказать взрослому, не отвечать, посоветоваться с родителями) и объяснить свой выбор.
- **Станция 5 «Вежливый чат» (тема 3.1):** команде выдаются карточки с фразами, нарушающими сетевой этикет (написаны КАПСЛОКОМ, содержат грубости, избыток смайлов). Задание: исправить фразу, сделав ее вежливой и понятной.

Подведение итогов:

- За каждое правильно выполненное задание команда получает фрагмент кода и от 1 до 5 баллов (в зависимости от полноты и правильности выполнения).
- В конце игры команды складывают из фрагментов общий код (пароль) и вводят его на «волшебном» компьютере (педагог проверяет правильность).
- Победителем становится команда, набравшая наибольшее количество баллов и правильно собравшая код.
- Параллельно педагог ведет индивидуальную карту наблюдения, отмечая активность и правильность ответов каждого обучающегося.

Критерии оценки

Уровень освоения программы	Характеристика
Высокий уровень	Обучающийся активно участвует в командной работе, правильно выполняет все задания, дает полные и аргументированные ответы, демонстрирует уверенное владение пройденным материалом.
Средний уровень	Обучающийся участвует в работе, выполняет большинство заданий правильно, но допускает незначительные ошибки или нуждается в помощи команды.
Допустимый уровень	Обучающийся выполняет задания с помощью педагога или других членов команды, допускает ошибки, путается в основных понятиях.
Низкий уровень	Обучающийся пассивен, не может выполнить задания даже с помощью, не ориентируется в пройденном материале.

Приложение 5. Диагностические материалы для подведения итогов реализации программы.

Диагностические материалы для подведения итогов реализации программы

Итоговая диагностика по программе «Цифровая безопасность» проводится на завершающих занятиях и направлена на комплексную оценку достижения планируемых результатов: предметных (знание правил и понятий), метапредметных (умение анализировать, применять знания в нестандартных ситуациях, работать с информацией) и личностных (ответственное отношение, эмпатия, самооценка). Диагностические материалы разработаны с учетом возрастных особенностей обучающихся 7–10 лет, включают игровые и наглядные элементы, исключают стрессовые ситуации.

Итоговая аттестация состоит из трех взаимодополняющих блоков:

1. **Защита итогового проекта** – демонстрация творческого продукта, отражающего знания и умения по выбранной теме.
2. **Решение проблемных кейсов** – комплексная проверка способности применять полученные знания в смоделированных ситуациях.
3. **Итоговое тестирование** – оценка усвоения основных понятий и правил.
4. **Диагностика личностных результатов** – педагогическое наблюдение и рефлексивные методики.

Блок 1. Итоговый тест «Знатоки цифровой безопасности»

Тест состоит из 20 заданий, охватывающих все разделы программы. Время выполнения – 30–35 минут (с учетом физкультминутки). Задания сопровождаются иллюстрациями (в реальной версии).

Инструкция для обучающихся: «Ребята, вы стали настоящими агентами кибербезопасности! Проверим, как вы готовы защищать себя и своих друзей в цифровом мире. Внимательно читайте вопросы, выбирайте правильные ответы. Некоторые задания нужно соединить стрелками или дописать слово. Удачи!».

Таблица 11.

№	Задание	Варианты ответов / Элементы для соединения	Правильный ответ
1	Как называется сеть, которая соединяет компьютеры по всему миру?	а) Интернет б) Программа в) Игра	а) Интернет
2	Какое устройство помогает выводить информацию на экран? (с картинками)	а) Клавиатура б) Монитор в) Мышь	б) Монитор

№	Задание	Варианты ответов / Элементы для соединения	Правильный ответ
3	Соедини стрелкой устройство и его назначение (картинки: принтер, наушники, колонки)	Печатать текст – принтер Слушать музыку – наушники Слушать звук – колонки	Верное соединение
4	Какая информация относится к персональным данным (её нельзя публиковать)? Выбери все правильные ответы.	а) Имя и фамилия б) Любимый цвет в) Домашний адрес г) Номер телефона	а, в, г
5	Какой пароль самый надежный?	а) 123456 б) qwerty в) Parol9!D	в) Parol9!D
6	Что нельзя делать, если в игре незнакомец просит прислать твою фотографию?	а) Посоветоваться с родителями б) Отправить фото, чтобы не обидеть в) Заблокировать его	б) Отправить фото
7	Как называется травля в Интернете, когда обижают, оскорбляют, дразнят?	а) Фишинг б) Кибербуллинг в) Вирус	б) Кибербуллинг
8	Что нужно сделать в первую очередь, если тебя начали травить в сети?	а) Ответить обидчику грубостью б) Не отвечать, сделать скриншот, рассказать взрослому в) Удалить свой аккаунт	б) Не отвечать, сделать скриншот, рассказать взрослому
9	Выбери правило сетевого этикета	а) Писать сообщения ЗАГЛАВНЫМИ БУКВАМИ б) Использовать вежливые слова в) Отправлять много смайлов, чтобы было весело	б) Использовать вежливые слова
10	Что такое фишинг?	а) Рыбалка в интернете б) Выуживание паролей и данных	б) Выуживание паролей и данных мошенниками

№	Задание	Варианты ответов / Элементы для соединения	Правильный ответ
		мошенниками в) Полезная игра	
11	На письме написано: «Вы выиграли приз! Перейдите по ссылке». Что делать?	а) Срочно перейти и получить приз б) Не переходить, спросить у родителей в) Отправить ссылку друзьям	б) Не переходить, спросить у родителей
12	Что такое вирус для компьютера?	а) Полезная программа б) Вредоносная программа, которая портит файлы в) Игрушка	б) Вредоносная программа
13	Как защитить компьютер от вирусов?	а) Установить антивирус и обновлять его б) Не включать компьютер в) Играть только в лицензионные игры	а) и в) (оба правильные, но тест может выбрать один; лучше указать: установить антивирус и играть в проверенные игры)
14	Сколько времени можно непрерывно работать за компьютером ребенку 7–10 лет?	а) 1 час б) 20–25 минут в) Сколько хочешь	б) 20–25 минут
15	Что нужно делать, чтобы глаза не уставали?	а) Сидеть близко к монитору б) Каждые 15–20 минут делать гимнастику для глаз в) Смотреть на яркий экран в темноте	б) Делать гимнастику для глаз
16	Выбери безопасную позу за компьютером (картинки: сутулый, ровная спина, лежа)		ровная спина
17	Можно ли верить всей информации, которую находишь в Интернете?	а) Да, ведь там всё написано правильно б) Нет, нужно проверять в других источниках и спрашивать взрослых	б) Нет, нужно проверять

№	Задание	Варианты ответов / Элементы для соединения	Правильный ответ
		в) Можно верить, если картинка красивая	
18	Что делать, если увидел в Интернете что-то страшное или неприличное?	а) Закрыть и забыть б) Рассказать родителям в) Поделиться с друзьями	б) Рассказать родителям
19	Можно ли добавлять в друзья всех подряд в социальных сетях?	а) Да, чем больше друзей, тем лучше б) Нет, только тех, кого знаешь в реальной жизни в) Можно, но только если у них красивая страница	б) Только тех, кого знаешь в реальной жизни
20	Если друг попросил твой пароль от игры, чтобы помочь пройти уровень, что ответить?	а) Конечно, мы же друзья! б) Нет, пароль нельзя давать никому, даже друзьям. Я лучше приду и помогу лично. в) Хорошо, но потом ты мне свой дашь.	б) Нет, пароль нельзя давать никому

Ключ к тесту:
1 – а; 2 – б; 3 – соединения верны; 4 – а,в,г; 5 – в; 6 – б; 7 – б; 8 – б; 9 – б; 10 – б; 11 – б; 12 – б; 13 – а; 14 – б; 15 – б; 16 – ровная спина; 17 – б; 18 – б; 19 – б; 20 – б.
Шкала оценивания:

- 18–20 правильных ответов – высокий уровень
- 14–17 правильных ответов – средний уровень
- 10–13 правильных ответов – допустимый уровень
- Менее 10 – низкий уровень (программа не освоена).

Блок 2. Итоговые проблемные кейсы

Обучающимся предлагается 4 комплексные ситуации, которые охватывают разные аспекты цифровой безопасности. Кейсы могут решаться индивидуально или в парах с последующим обсуждением. Каждый кейс оценивается по 5-балльной шкале (критерии ниже).

Кейс 1. «Подарок от незнакомца»

Ситуация: «В мессенджер Даше пришло сообщение от незнакомого человека: "Привет! Ты выиграла супер-приз – новый телефон! Чтобы его получить, нужно перейти по ссылке и ввести свои данные: имя, адрес, номер телефона. Ссылка уже здесь". Даша очень обрадовалась, ведь она мечтала о новом телефоне. Но вспомнила наши уроки и задумалась...»

Вопросы:

1. Почему Даша задумалась? Какие признаки обмана она могла заметить?
2. Что произойдет, если перейти по ссылке и ввести данные?
3. Как правильно поступить Даше?
4. Что бы ты посоветовал Даше, чтобы она не попадалась на такие уловки в будущем?

Правильные ориентиры:

1. Признаки: незнакомый отправитель, неожиданный выигрыш (Даша нигде не участвовала), просьба перейти по ссылке и ввести личные данные, слишком щедрое предложение.
2. Последствия: потеря личных данных, кража аккаунтов, деньги с карты родителей (если данные), заражение устройства вирусом.
3. Не переходить по ссылке, не вводить данные, показать сообщение родителям, заблокировать отправителя.
4. Совет: всегда советоваться с родителями, не доверять «халяве», проверять информацию, помнить правила.

Кейс 2. «Ссора в чате класса»

Ситуация: «В чате класса одноклассники обсуждали домашнее задание. Вдруг Миша написал: "Петя вечно тупит, его ответы никому не нужны". Петя обиделся и написал грубость в ответ. Началась перепалка, к ней присоединились ее знакомые. Чат превратился в место ссоры. Маша, староста класса, хотела помирить всех, но не знала как».

Вопросы:

1. Как называется такое поведение в сети?
2. Кто начал конфликт? Кто прав, кто виноват?
3. Какие правила сетевого этикета нарушили ребята?
4. Что нужно сделать, чтобы остановить ссору?
5. Как правильно поступить Маше? Какой алгоритм действий ты предложишь?

Правильные ориентиры:

1. Кибербуллинг (начальная стадия), провокация, троллинг.
2. Начал Миша – он оскорбил Петю. Оба повели себя неправильно (ответная грубость).
3. Нарушили: уважение к собеседнику, правило «не писать то, что обидит», не давать волю эмоциям.
4. Остановить: напомнить о правилах, предложить прекратить переписку, перевести обсуждение в личные сообщения.

5. Маше: написать в чат, что так общаться нельзя, попросить всех успокоиться, предложить обсудить проблему лично с учителем, при необходимости пригласить взрослого.

Кейс 3. «Загадочный друг»

Ситуация: «В онлайн-игре к Диме добавился новый персонаж – "Волшебник". Он написал: "Привет! Я тоже учусь в 3 классе. Хочу подарить тебе крутой скин. Скажи свой логин и пароль от игры, я его активирую". Дима обрадовался, но почувствовал что-то неладное».

Вопросы:

1. Почему Дима насторожился? Что его должно было смутить?
2. Почему нельзя сообщать логин и пароль от игры даже за подарки?
3. Как правильно ответить «Волшебнику»?
4. Что может случиться, если Дима всё же отправит пароль?
5. Какую пользу извлек Дима из этого случая?

Правильные ориентиры:

1. Смутило: просьба дать пароль (никогда нельзя давать), слишком щедрое предложение, незнакомый персонаж.
2. Пароль – это ключ к аккаунту. Получив его, мошенник может украсть аккаунт, удалить достижения, написать от твоего имени.
3. Ответ: отказаться, сказать, что пароль – личная тайна, и родители запрещают его сообщать; заблокировать незнакомца.
4. Потеря аккаунта, деньги, если к аккаунту привязана карта, использование аккаунта для мошенничества.
5. Дима понял, что не всем можно доверять, и запомнил правило «никогда не сообщай пароль».

Кейс 4. «Игра до ночи»

Ситуация: «Катя очень любит компьютерные игры. В пятницу вечером она села поиграть на часок, а когда подняла голову, на часах было уже 11 ночи. Родители легли спать, а Катя даже не сделала уроки. На следующий день у неё болела голова и слипались глаза. А в понедельник она получила двойку за невыученное стихотворение».

Вопросы:

1. Какая проблема возникла у Кати?
2. Почему нельзя играть так долго? К каким последствиям это приводит?
3. Что такое «цифровая зависимость»? Есть ли она у Кати?
4. Составь для Кати правила, которые помогут ей контролировать время за компьютером.
5. Как родители могут помочь Кате?

Правильные ориентиры:

1. Проблема: игровая зависимость, нарушение режима, ухудшение здоровья, снижение успеваемости.
2. Последствия: усталость глаз, головная боль, плохой сон, невыполненные уроки, ссоры с родителями.

3. Цифровая зависимость – когда не можешь оторваться от игры, забываешь обо всём. У Кати есть признаки зависимости.
4. Правила: ставить таймер на 30 минут; делать перерывы; сначала уроки – потом игры; договариваться с родителями о времени; гулять и заниматься спортом.
5. Родители могут установить родительский контроль, контролировать время, предлагать альтернативные занятия.

Критерии оценки решения кейсов (по каждому кейсу):

Таблица 12

Уровень	Баллы	Характеристика
Высокий	5	Обучающийся правильно определяет проблему, видит все признаки опасности, предлагает полный и безопасный алгоритм действий, аргументирует, проявляет критическое мышление.
Средний	4	Обучающийся в целом верно понимает ситуацию, называет основные ошибки и правильные действия, но может упустить некоторые детали или недостаточно аргументировать.
Допустимый	3	Обучающийся определяет только явную угрозу, называет одно-два правильных действия, но не видит скрытых рисков, аргументация слабая.
Низкий	1–2	Обучающийся не понимает сути ситуации, предлагает опасные варианты, не может объяснить выбор.

Максимальная сумма за 4 кейса – 20 баллов.

Блок 3. Защита итогового проекта

Обучающиеся самостоятельно выбирают тему из предложенного списка или предлагают свою, согласованную с педагогом. Формы проекта: презентация, памятка, буклет, комикс, плакат, настольная игра, видеоролик, интерактивный тест.

Темы проектов (примерный перечень):

1. «Правила безопасного Интернета для первоклассников»
2. «Как создать надежный пароль и не забыть его»
3. «Что нельзя публиковать в соцсетях»
4. «Кибербуллинг: как защитить себя и друга»
5. «Фишинг и как его распознать»
6. «Мой безопасный цифровой день»
7. «Энциклопедия цифровых угроз для детей»
8. «Правила этикета в мессенджерах»
9. «Здоровье за компьютером: памятка для одноклассников»
10. «Как не попасть в ловушку мошенников в игре»

Критерии оценки итогового проекта (максимум 15 баллов)

Таблица 13

Критерий	Показатели	Баллы
Соответствие теме	Тема раскрыта полно, содержание соответствует заявленной проблеме	0–3
Правильность содержания	Все правила и рекомендации изложены верно, отсутствуют ошибки	0–3
Самостоятельность выполнения	Проект выполнен самостоятельно (допустима помощь педагога на этапе консультации)	0–3
Творческий подход	Оригинальность идеи, нестандартное оформление, авторские находки	0–3
Качество представления	Четкость, логичность, умение ответить на вопросы, уверенность	0–3
ИТОГО		**15**

Уровни освоения по итогам проекта:

- 13–15 баллов – высокий уровень
- 9–12 баллов – средний уровень
- 5–8 баллов – допустимый уровень
- менее 5 баллов – низкий уровень (требуется доработка)

Блок 4. Диагностика личностных результатов

Личностные результаты оцениваются методом педагогического наблюдения в процессе занятий, игр, проектной деятельности, а также через рефлексивные методики.

4.1. Карта педагогического наблюдения

Педагог наблюдает за каждым обучающимся в течение всего периода обучения и фиксирует проявления по следующим параметрам (заполняется в конце года):

Таблица 14

ФИО	Параметры наблюдения	Уровень проявления (высокий/средний/низкий)
	Проявляет ответственное отношение к личной информации (не разглашает, использует сложные пароли)	
	Демонстрирует эмпатию, поддерживает других в ситуациях кибербуллинга	
	Соблюдает правила цифрового этикета	
	Способен самостоятельно принимать решения в ситуациях онлайн-риска	
	Проявляет интерес к теме, активно участвует в обсуждениях	
	Осознаёт последствия своих действий в сети	
	Умеет обратиться за помощью к взрослым в сложных ситуациях	

Шкала оценки: 3 балла – высокий, 2 – средний, 1 – низкий.

4.2. Анкета «Я в цифровом мире» (рефлексивная методика)

Проводится на итоговом занятии. Обучающимся предлагается ответить на вопросы (можно в виде рисунка или выбора варианта).

Инструкция: «Ответь на вопросы честно. Если согласен с утверждением, поставь ✓, если нет – ✗».

1. Я знаю, что такое персональные данные, и никогда не публикую их в интернете.
2. У меня есть надежные пароли, и я никому их не даю.
3. Если ко мне в сети обратится незнакомец, я расскажу об этом родителям.
4. Я знаю, как вести себя, если столкнулся с кибербуллингом.
5. Я стараюсь соблюдать правила вежливости в интернете.
6. Я проверяю информацию, прежде чем поверить ей.
7. Я соблюдаю режим работы за компьютером, делаю зарядку для глаз.
8. Я готов помочь другу, если у него возникли проблемы в интернете.
9. После наших занятий я стал(а) более осторожным(ой) в интернете.

10. Мне было интересно изучать цифровую безопасность.

Обработка: подсчет положительных ответов. 9–10 положительных ответов – высокий уровень личностного развития; 7–8 – средний; 5–6 – допустимый; менее 5 – низкий (требуется дополнительная работа).

4.3. Методика «Неоконченные предложения»

Дополняет анкету, позволяет выявить ценностные установки. Обучающиеся дописывают предложения:

- В интернете я боюсь...
- Если бы меня обижали в сети, я бы...
- Мои родители знают, что я...
- Самое главное правило безопасности – это...
- Я хочу научиться...

Анализ ответов позволяет увидеть изменения в восприятии цифровых рисков и сформированные ценностные ориентиры.

Блок 5. Сводная ведомость результатов подведения итогов реализации программы

По окончании программы заполняется сводная ведомость на каждого обучающегося и на группу в целом.

Таблица 15

ФИО	Итоговый тест (баллы/уровень)	Решение кейсов (баллы/уровень)	Проект (баллы/уровень)	Личностные результаты (наблюдение + анкета)	Итоговый уровень освоения программы

Итоговый уровень освоения программы определяется как среднее арифметическое по четырем блокам (перевод в уровни: высокий, средний, допустимый, низкий).

Критерии итогового уровня:

- **Высокий уровень:** обучающийся демонстрирует глубокие знания, уверенно применяет их в нестандартных ситуациях, проявляет самостоятельность, ответственность и эмпатию, творчески подходит к решению задач.
- **Средний уровень:** обучающийся освоил программу, знает основные правила, но может испытывать затруднения в сложных ситуациях, нуждается в эпизодической помощи.
- **Допустимый уровень:** обучающийся усвоил базовые понятия, но допускает ошибки, не всегда применяет правила на практике, требует контроля и напоминаний.
- **Низкий уровень:** программа не освоена, знания фрагментарны, навыки безопасного поведения не сформированы.

Рекомендации по оформлению результатов:

- результаты фиксируются в индивидуальной карте обучающегося;
- сводная ведомость сдается в методический кабинет;
- лучшие проекты рекомендуются для участия в конкурсах по кибербезопасности;
- родители информируются об итогах освоения программы на родительском собрании или в индивидуальных беседах.

Приложение 6. Договор о сетевой форме взаимодействия

Договор
о сетевой форме реализации образовательных программ

г.Ростов-на-Дону "____" августа 202_ г.

Муниципальное бюджетное учреждение дополнительного образования Железнодорожного района г.Ростова-на-Дону, осуществляющее образовательную деятельность на основании лицензии от 05.12.2017 г. серия 61Л01 №0004375, выданной Ростобрнадзором , именуемое в дальнейшем "Базовая организация", в лице директора Андреевой Натальи Николаевны, действующей на основании Устава, с одной стороны, и, **муниципальное бюджетное общеобразовательное учреждение города Ростова-на-Дону "Школа № 83 имени Героя Российской Федерации Казанцева В.Г.,** именуемое в дальнейшем "Организация-участник", в лице директора **Галстяна Арсена Кареновича**, действующего на основании Устава, с другой стороны, именуемые по отдельности "Сторона", а вместе - "Стороны", заключили настоящий договор (далее - Договор) о нижеследующем.

1. Предмет Договора

1.1. Предметом настоящего Договора является реализация Сторонами дополнительной общеразвивающей программы «Цифровая безопасность» технической направленности, стартового уровня, с использованием сетевой формы (далее соответственно - сетевая форма, Образовательная программа).

1.2. Образовательная программа утверждается Базовой организацией.

1.3. Образовательная программа реализуется в период с 01.09.202__ г. по 31.05.202__г.

2. Осуществление образовательной деятельности при реализации Образовательной программы

2.1. Образовательная программа «Цифровая безопасность» реализуется Базовой организацией, ее объем и содержание определяются Образовательной программой и настоящим Договором.

2.2. Организация-участник предоставляет следующие ресурсы, необходимые для реализации Образовательной программы: помещение, оборудование, материалы для реализации программы (далее - Ресурсы), в части программы, представленной учебным планом, приложение 1.

2.3. Базовая организация предоставляет кадровые ресурсы, необходимые для реализации Образовательной программы.

2.4. Число обучающихся по Образовательной программе (далее обучающиеся) составляет от 10 до 12 человек. Поименный список обучающихся направляется Базовой организацией в Организацию-участник не менее чем за 14 рабочих дней до начала реализации Образовательной программы, указанных в пункте 1.3 настоящего Договора.

2.5. Организация-участник не позднее 5 рабочих дней с момента заключения настоящего Договора определяет лицо, ответственное за взаимодействие с Базовой организацией по предоставлению Ресурсов.

Об изменении указанного в настоящем пункте ответственного лица Организация-участник должна незамедлительно проинформировать Базовую организацию.

2.6. Закупку расходных материалов осуществляет Базовая организация.

2.7. Организация рабочего места для обучающегося осуществляет Организация-участник.

2.8. Предоставление оборудования для реализации Образовательной программы осуществляют как Базовая организация, так и организация-участник.

2.9. Базовая организация предоставляет педагогов дополнительного образования и педагогов-организаторов.

2.10. Предоставление методических материалов осуществляет Базовая организация.

2.11. Освоение обучающимися Образовательной программы в Организации-участнике сопровождается осуществлением текущего контроля успеваемости проводимого в формах, определенных учебным планом Образовательной программы, и в порядке, установленном локальными нормативными актами Базовой организации.

2.12. По запросу Базовой организации Организация-участник должна направить информацию о посещении обучающимися учебных и иных занятий, текущем контроле успеваемости в срок не позднее 3-х рабочих дней с момента получения запроса.

2.13. Подведение итогов реализации программы проводится Базовой организацией.

2.14. Обучающимся, успешно усвоившим Образовательную программу Базовой организацией выдается Свидетельство выпускника муниципального бюджетного учреждения дополнительного образования Железнодорожного района г.Ростова-на-Дону.

2.15. Базовая организация вправе проверять условия предоставления помещения и оборудования, не нарушая автономию Организации-участника.

3. Финансовое обеспечение реализации Образовательной программы

3.1. Базовая организация осуществляет финансовое обеспечение реализации Образовательной программы.

3.2. Организация-участник предоставляет ресурсы, оборудование и материалы на безвозмездной основе.

4. Срок действия Договора

4.1. Настоящий Договор вступает в силу со дня его заключения.

4.2. Настоящий Договор заключен на период реализации Образовательной программы, предусмотренный пунктом 1.3 настоящего Договора.

5. Заключительные положения

5.1. Условия, на которых заключен Договор, могут быть изменены по соглашению Сторон или в соответствии с законодательством Российской Федерации.

5.2. Договор может быть расторгнут по соглашению Сторон или в судебном порядке по основаниям, предусмотренным законодательством Российской Федерации.

5.3. Действие Договора прекращается в случае прекращения осуществления образовательной деятельности Базовой организации, приостановления действия или аннулирования лицензии на осуществление образовательной деятельности Базовой организации, прекращения деятельности Организации-участника.

5.4. Все споры, возникающие между Сторонами по настоящему Договору, разрешаются Сторонами в порядке, установленном законодательством Российской Федерации.

5.5. Настоящий Договор составлен в 2-х экземплярах, по одному для каждой из сторон. Все экземпляры имеют одинаковую юридическую силу. Изменения и дополнения настоящего Договора могут производиться только в
письменной форме и подписываться уполномоченными представителями Сторон.

5.6. К Договору прилагаются и являются его неотъемлемой частью:
приложение N 1 - Ресурсы Организации-участника.

Адреса, реквизиты и подписи Сторон

Базовая организация	Организация-участник
муниципальное бюджетное учреждение дополнительного образования Железнодорожного района г.Ростова-на-Дону «Дом детского творчества» г.Ростов-на-Дону ул. Верещагина, д. 10 Директор Андреева Наталья Николаевна _____ «____»_____202___г. М.П.	муниципальное бюджетное общеобразовательное учреждение города Ростова-на-Дону "Школа № 83» имени Героя Российской Федерации Казанцева В.Г., г.Ростов-на-Дону пр-кт Ставского, д. 33 Директор Галстян Арсен Каренович _____ «____»_____202___г. М.П.

Приложение 1.

Ресурсы Организации-участника

№ п/п	Наименование ресурсов организации – участника на реализацию образовательной программы	Кол-во
1.	Персональный компьютер (системный блок, монитор, клавиатура, мышь)	12 шт.
2.	Ноутбук для педагога	1 шт.
3.	Многофункциональное устройство (принтер, сканер, копир)	1 шт.
4.	Интерактивная доска или интерактивная панель (диагональ не менее 165,1 см)	1 шт.
5.	Проектор с экраном	1 комплект
6.	Акустическая система (колонки)	2 шт.
7.	Наушники с микрофоном	12 комплектов
8.	Компьютерный стол (одноместный)	12 шт.
9.	Стул компьютерный регулируемый	12 шт.
10.	Парта двухместная для теоретических занятий	6 шт.
11.	Стул ученический	12 шт.
12.	Магнитно-маркерная доска	1 шт.
13.	Лицензионная операционная система	на все ПК
14.	Пакет офисных программ (текстовый редактор, редактор презентаций)	на все ПК
15.	Простой графический редактор (Paint, Tux Paint)	на все ПК
16.	Безопасный браузер с системой контент-фильтрации	на все ПК
17.	Лицензионное антивирусное программное обеспечение	на все ПК
18.	Учебные тренажеры-симуляторы по цифровой безопасности (онлайн или локальные)	на все ПК

№ п/п	Наименование ресурсов организации – участника на реализацию образовательной программы	Кол-во
19.	Бумага для печати (формат А4)	5 пачек
20.	Бумага цветная (формат А4)	5 наборов
21.	Картон цветной	5 наборов
22.	Ватманы (формат А1, А2)	20 шт.
23.	Фломастеры, маркеры, цветные карандаши	15 комплектов
24.	Краски (гуашь, акварель), кисти	5–6 наборов
25.	Клей-карандаш, клей ПВА	15–20 шт.
26.	Ножницы с закругленными концами	15 пар
27.	Сетевой фильтр (удлинитель с заземлением)	5–6 шт.
28.	Доступ к сети Интернет с контент-фильтрацией	1
29.	Учебные кабинеты (компьютерные классы) для проведения занятий	1
30.	Помещения для проведения теоретических занятий и творческих мастерских	1