АДМИНИСТРАЦИЯ БАГАНСКОГО РАЙОНА НОВОСИБИРСКОЙ ОБЛАСТИ

МУНИЦИПАЛЬНОЕ КАЗЁННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ — КАЗАНСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА

Рассмотрена и одобрена **на заседании педагогического совета** **протокол № 1** **« 28 » августа 2026 г.**	**УТВЕРЖДАЮ** **Директор МКОУ-Казанская СОШ** **П.В. Зейбель** **(подпись)** **М.П.** **Приказ № 215-ОД от 31.08.2026г.**

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

Стартовый уровень
технической направленности

«Кибербезопасность»

Возраст обучающихся: 10–12 лет

Срок реализации программы: 1 год (34 недели)

Автор – составитель программы:
Зейбель П.В., педагог дополнительного образования
МКОУ-Казанская СОШ

Программу реализует:
Зейбель П.В., учитель информатики
МКОУ-Казанская СОШ

с. Казанка, 2026

Внутренняя экспертиза проведена. Программа рекомендована к рассмотрению на педагогическом совете учреждения.

Зам. директора ОУ по УВР / Методист  Азарова М.В. «31» августа 2026 г.

Содержание

Раздел 1. Комплекс основных характеристик программы 1
1.1. Пояснительная записка 1
Направленность программы 1
Актуальность 1
Отличительные особенности ДОП, новизна 1
Целевая аудитория (адресат программы) 2
Объём программы 2
Срок реализации программы 3
Форма обучения 3
Уровень программы 3
Форма реализации образовательной программы 3
Режим занятий 2
Язык обучения 3
Запись на программу 3
1.2. Цель и задачи программы 3
Личностные задачи 4
Метапредметные задачи 4
Предметные задачи 4
1.3. Планируемые результаты 4
Личностные результаты 4
Метапредметные результаты 5
Предметные результаты 6
1.4. Содержание программы 7
Структура модулей 7
Учебный план 7
Содержание учебного плана (34 часа) 9
Модуль 1. Цифровой мир и интернет-зависимость 8
Модуль 2. Техносфера и технические риски 8
Модуль 3. Информация и контентные риски 8
Модуль 4. Общение и коммуникационные риски 8
Модуль 5. Цифровая экономика и потребительские риски 8
Модуль 6. Персональные данные 8
Модуль 7. Цифровое будущее 8
1.5. Система контроля и формы аттестации 13
Система контроля 13
Виды контроля и аттестации 14
Критерии оценки для итоговой аттестации 14
Оценочные материалы (общая характеристика) 14
Диагностические методики и задания по группам результатов 15
Комплект диагностических материалов с игровыми и наглядными формами 18
Критерии оценки проектного задания 18
Обеспечение объективности и надёжности 19

Раздел 2. Рабочая программа воспитания 19
2.1. Цель, задачи и целевые ориентиры воспитания 19
Цель воспитания 19
Задачи воспитания 19
Целевые ориентиры воспитания 20
2.2. Формы и методы воспитания 20
Формы воспитательной работы 20
Методы воспитания 21
2.3. Условия организации воспитания 21
Воспитывающая среда 21
Педагогические условия 21
Организационные условия 22
2.4. Календарный план воспитательной работы 22
2.5. Результативно-диагностическая часть (ожидаемые результаты воспитания) 25
2.6. Связь рабочей программы воспитания с программой курса 25
Раздел 3. Комплекс организационно-педагогических условий 26
3.1. Календарный учебный график 26
Общие параметры учебного года 26
Календарный учебный график (на одну группу) 26
График проведения аттестационных процедур 27
3.2. Условия реализации программы 27
Материально-техническое обеспечение 27
Кадровое обеспечение 28
Информационное обеспечение (интернет-ресурсы) 28
3.3. Методическое обеспечение 28
Учебно-методическое обеспечение 28
Перечень методических разработок для педагога 29
Рекомендации по организации образовательного процесса 29
3.4. Список литературы для педагога 29
3.5. Список литературы для обучающихся 30
3.6. Нормативная база 30
Приложения 31
Приложение 1. Календарный учебный график на 2025–2026 учебный год 31
Приложение 2. Оценочные (контрольно-измерительные) материалы 34
2.1. Входная диагностика 34
2.2. Итоговый тест (15 вопросов) 34
2.3. Анкета для оценки личностных результатов «Я в Интернете» 36
2.4. Критерии оценки проекта «Школа будущего» 36
2.5. Карта наблюдения за метапредметными результатами (экспертная карта) 37
Приложение 3. Перечни оборудования и средств обучения, дидактических материалов 37
3.1. Оборудование и технические средства 37
3.2. Программное обеспечение и цифровые ресурсы 37
3.3. Дидактические материалы (раздаточные) 38
3.4. Учебно-методическая литература (на группу) 38

Раздел 1. Комплекс основных характеристик программы

1.1. Пояснительная записка

Дополнительная общеразвивающая программа «Кибербезопасность» разработана для формирования у обучающихся базовых знаний и практических навыков безопасного поведения в цифровой среде.

Направленность программы

Направленность программы: техническая

Актуальность

Социальная среда, в которой растут современные дети, значительно отличается от той, что формировала их родителей. Цифровые технологии проникают во все аспекты жизни, формируя цифровое общество, где Интернет становится важным фактором социализации.

Компьютер, подключённый к Интернету, расширяет зону ближайшего развития ребёнка — область созревающих психических функций и образовательного потенциала. Однако социализация в Интернете часто стихийна и неконтролируема, дети осваивают технологии самостоятельно, что увеличивает риски.

Интернет, несмотря на доверие к нему, представляет опасность из-за отсутствия жизненного опыта у детей для оценки рисков. Взрослые должны стать проводниками в цифровом мире, обучая детей безопасному использованию Интернета.

Школа несёт ответственность за развитие цифровой компетентности и навыков безопасного поведения в киберпространстве. Важно воспитывать «цифрового гражданина», обладающего техническими навыками и критическим мышлением.

Программа по цифровой компетентности востребована из-за:

- Интернета как важного фактора социализации;
- активного использования Интернета детьми в образовательных целях;
- требований современной среды к цифровой компетентности;
- самостоятельного и бессистемного освоения технологий детьми;
- роли школы в цифровой социализации.

Отличительные особенности ДОП, новизна

1. Модульная структура.

Курс состоит из семи модулей (от «Цифрового мира и интернет-зависимости» до «Цифрового будущего»). При этом содержание модулей постепенно усложняется, что позволяет углублять знания и навыки год от года.

2. Сквозные персонажи и игровая форма подачи.

Введены персональные помощники (Кибернешка, магистр Кибер Нетов, профессор Кибер Нетович), а также школьники с разными типами поведения (Гоша Геймеров — любитель игр, Рита Картинкина — общительный пользователь, Игорь Неюзеров —

искатель информации). Текст оформлен как «посты» в социальной сети с хештегами — это повышает мотивацию и приближает материал к реальному опыту подростков.

3. Охват всех основных видов онлайн-рисков.

Программа системно рассматривает пять категорий рисков: технические, контентные, коммуникационные, потребительские и риск интернет-зависимости. Для каждой группы предлагаются конкретные стратегии безопасного поведения и способы разрешения проблемных ситуаций.

4. Акцент на формирование позитивного образа цифрового будущего.

В отличие от многих курсов, которые фокусируются только на угрозах, в программе выделен отдельный модуль 7 «Цифровое будущее». Он направлен на создание позитивного, конструктивного образа цифровых технологий, помощь в планировании жизненного пути и реализации личностного потенциала в цифровом обществе.

5. Широкий спектр форм деятельности и вариативность заданий.

Занятия предполагают не только лекции, но и индивидуальную, парную, групповую работу, дискуссии, круглые столы, дебаты. Задания имеют разные форматы (тетрадь, цифровые устройства, интерактив), что позволяет переключать виды деятельности и соблюдать здоровьесберегающие принципы.

6. Курс реализуется за счёт вариативной части учебного плана.

Программа рассчитана на 1 час в неделю (34 часа в год) и может вестись не только учителями информатики, но и классными руководителями, педагогами-психологами, социальными педагогами, педагогами дополнительного образования.

7. Практико-ориентированное распределение часов.

В тематическом планировании указано не только общее количество часов, но и деление на аудиторные и практические занятия. Это подчёркивает активную, деятельностную направленность курса.

Целевая аудитория (адресат программы)

Адресат: обучающиеся 10–11 лет общеобразовательных организаций.

- Обоснование: возраст активной и бессистемной цифровой социализации, высокая уязвимость к онлайн-рискам, необходимость формирования зоны ближайшего развития в цифровой среде.
- Особые потребности: программа не специализирована, но адаптируема для детей с ОВЗ, одарённых, детей в ТЖС (нет противопоказаний).
- Формирование групп: по классам (параллелям), без отбора по уровню подготовки, возможен смешанный состав.
- Условия приёма: свободный набор, без собеседования, при наличии технических средств.

Объём программы

Объём	Срок освоения	Режим занятий
34 часа	1 учебный год (34	1 раз в неделю по 1 академическому часу.

	недели)	Продолжительность одного академического часа — 45 минут, при электронном обучении или обучении с применением дистанционных технологий — 30 минут.

Срок реализации программы

Срок реализации ДОП: 1 учебный год (34 недели).

Форма обучения

Форма обучения: очная — традиционная форма обучения, включает теоретические (не более 30%) и практические (не менее 70%) занятия, организованные по времени вне основного образования.

Уровень программы

Уровень ДОП: стартовый.

Форма реализации образовательной программы

Формы реализации ДОП: традиционная форма обучения.

Режим занятий

Режим занятий: 1 раз в неделю по 1 академическому часу. Продолжительность одного академического часа — 45 минут, при электронном обучении или обучении с применением дистанционных технологий — 30 минут.

Язык обучения

Язык обучения — русский.

Запись на программу

Запись на дополнительную общеобразовательную общеразвивающую программу осуществляется через систему заявок на сайте ГИС «Навигатор дополнительного образования детей Новосибирской области» (https://navigator.edu54.ru/). Приказ министерства образования Новосибирской области от 19.09.2023 № 2064 «Об утверждении положения о государственной информационной системе «Навигатор дополнительного образования Новосибирской области». https://navigator.edu54.ru

1.2. Цель и задачи программы

Освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства, а также эффективно распознавать, предотвращать и разрешать проблемные ситуации, связанные с основными видами онлайн-рисков.

Задачи

Личностные задачи

Направлены на воспитание ответственного, осознанного и этичного пользователя, развитие личных качеств и мотивации.

1. Вырабатывать сознательное и бережное отношение к вопросам собственной информационной безопасности и защите персональных данных.

2. Формировать и развивать нравственные, этические качества личности, включая ответственность за свои действия в цифровой среде и соблюдение норм информационной этики.

3. Стимулировать познавательную активность и поведение, направленные на соблюдение правил информационной безопасности и профилактику интернет-зависимости.

Метапредметные задачи

Ориентированы на развитие универсальных компетенций, которые выходят за рамки предмета и применимы в различных жизненных и учебных ситуациях.

1. Развивать компьютерную грамотность и информационную культуру личности, необходимые для эффективного и безопасного использования информационных и коммуникационных технологий.

2. Развивать умения анализировать, систематизировать и критически осмысливать получаемую информацию, выявляя недостоверные или потенциально опасные данные.

3. Развивать познавательную и творческую активность, а также навыки проектной деятельности для безопасного применения цифровых технологий в решении практических задач.

Предметные задачи

Направлены на приобретение конкретных знаний, умений и компетенций в области кибербезопасности («жёстких» навыков).

1. Способствовать формированию знаний о безопасном поведении при работе с компьютерными программами и информацией в сети Интернет.

2. Формировать умения соблюдать нормы информационной этики и права, а также безопасно использовать средства коммуникации для защиты от мошенничества.

3. Формировать умения безопасно работать с информацией, анализировать и обобщать ее, а также применять практические навыки защиты личных устройств и данных (например, создание надёжных паролей, распознавание угроз).

1.3. Планируемые результаты

Освоение программы направлено на достижение личностных, метапредметных и предметных результатов.

Личностные результаты

Связаны с ценностно-смысловыми установками, мотивацией и развитием качеств личности в процессе освоения программы.

Мотивационный компонент

У обучающегося будет сформировано:

- осознанное стремление к личностному росту и самореализации в цифровой среде;
- потребность в безопасном и ответственном использовании Интернета;
- интерес к освоению новых цифровых технологий (искусственный интеллект, умный город, интернет вещей) и их применению в учёбе, быту, будущей профессии;
- желание участвовать в социально значимых онлайн-проектах, распространять культуру кибербезопасности среди сверстников.

Личностные качества и ценностные установки

В ходе курса у обучающегося будут развиты:

- ответственность — за свои действия в Интернете, за сохранность персональных данных, за репосты и распространяемую информацию;
- самостоятельность — способность принимать решения в проблемных ситуациях, не поддаваясь панике или давлению;
- критичность — здоровое недоверие к подозрительным ссылкам и незнакомцам, умение отличать факты от мнений;
- эмпатия и уважение — доброжелательное отношение к другим пользователям, нетерпимость к кибербуллингу, троллингу, агрессии, готовность поддержать жертву;
- дисциплинированность — соблюдение баланса между онлайн и офлайн, способность контролировать время в Сети, противостоять интернет-зависимости;
- правосознание — уважение к авторскому праву, законодательству о персональных данных, нетерпимость к пиратству и плагиату;
- активная жизненная позиция — готовность созидать позитивный цифровой контент, участвовать в создании безопасной онлайн-среды, в том числе через социальную рекламу и волонтёрские проекты.

Метапредметные результаты

Ориентированы на формирование универсальных учебных действий (УУД) и гибких навыков, применимых в любых сферах жизни.

Предметные результаты

Отражают систему теоретических знаний и практических умений в области кибербезопасности, соответствующих семи модулям курса.

Знания (теоретический компонент)

Обучающийся будет знать:

- основные виды онлайн-рисков: технические (вирусы, вредоносные программы), контентные (неприемлемый контент, фейки), коммуникационные (троллинг, кибербуллинг, общение с незнакомцами), потребительские (мошенничество, фишинг, спам) и риск интернет-зависимости;

- понятия: персональные данные, цифровой след, приватность, авторское право, лицензии (Creative Commons и др.), криптовалюта, искусственный интеллект, дополненная и виртуальная реальность;
- правила безопасного подключения к Интернету (проводное/беспроводное), требования к надёжному паролю, способы защиты устройств от вирусов;
- принципы работы поисковых систем, критерии достоверности информации, признаки фейковых новостей;
- нормативно-правовые основы: основные положения ФЗ «О персональных данных», «О защите детей от информации, причиняющей вред», статьи ГК РФ об авторском праве.

Умения (практический компонент)

Обучающийся сможет:

- настраивать безопасный поиск, использовать кнопку «пожаловаться на контент», управлять всплывающими окнами и доступом к геолокации/камере/микрофону в браузере;
- составлять и хранить надёжные пароли, использовать режим инкогнито, настраивать приватность в социальных сетях, удалять цифровые следы;
- распознавать фишинговые сайты, подозрительные ссылки и вложения, мошеннические СМС;
- проверять информацию на достоверность (фактчекинг), отличать фейковые новости и изображения от подлинных;
- применять алгоритмы действий при кибербуллинге, троллинге, столкновении с неприятным контентом: не отвечать агрессией, сохранять доказательства, заблокировать обидчика, обратиться за помощью к взрослым или в службу поддержки;
- соблюдать авторские права при использовании чужих материалов, выбирать легальные источники контента;
- безопасно совершать онлайн-покупки: проверять надёжность интернет-магазина, избегать подозрительных баннеров, использовать защищённые платёжные инструменты;
- управлять своей онлайн-репутацией: контролировать публикуемую информацию, отвечать на отзывы, удалять нежелательные материалы;
- использовать облачные сервисы и локальные приложения с учётом их плюсов и минусов.

1.4. Содержание программы

Программа реализуется в течение 1 года. 1 час в неделю (34 часа в год).

Содержание построено по модульному принципу. Каждый учебный год включает 7 одинаковых по названию модулей, которые постепенно усложняются. Модули 1–6 отражают основные области возможностей и рисков в Интернете, модуль 7 формирует позитивный образ цифрового будущего.

Структура модулей

№ модуля	Название модуля	Основное содержание
1	Цифровой мир и интернет-зависимость	История Интернета, типы пользователей, признаки зависимости, баланс времени.
2	Техносфера и технические риски	Устройство Интернета, программное обеспечение, вирусы, пароли, безопасное подключение.
3	Информация и контентные риски	Поиск информации, достоверность, фейки, авторское право, неприемлемый контент.
4	Общение и коммуникационные риски	Сервисы общения, правила нетикета, кибербуллинг, троллинг, безопасная коммуникация.
5	Цифровая экономика и потребительские риски	Онлайн-покупки, реклама, мошенничество, фишинг, электронные платежи.
6	Персональные данные	Что такое персональные данные, цифровой след, настройки приватности, управление репутацией.
7	Цифровое будущее	Дополненная/виртуальная реальность, искусственный интеллект, умный город, профессии будущего.

Учебный план

№	Название темы	Всего часов	Теория	Практика	Формы аттестации / контроля
Модуль 1. Цифровой мир и интернет-зависимость (3 часа)					
1	Тема 1. Зачем нам нужен Интернет	3	1	–	мини-тест «Типы пользователей», рефлексивный дневник времени в Сети
Модуль 2. Техносфера и технические риски (4 часа)					
2	Тема 2. Как устроен Интернет	4	2	2	Практическая работа: настройка браузера, установка антивируса (в симуляции), кейс «Вирусная атака»
Модуль 3. Информация и контентные риски (8 часов)					
3	Тема 3. Какая бывает информация	4	2	2	Заполнение таблицы «Виды информации», практика: измерение объёма данных
4	Тема 4. Как работает поиск в Интернете	4	2	2	Практическое задание: построение поисковых запросов, настройка безопасного поиска, кейс «Найди фейк»
Модуль 4. Общение и коммуникационные риски (4 часа)					
5	Тема 5. Как люди общаются в Интернете	4	2	2	Ролевая игра «Правила нетикета», анализ ситуаций общения с незнакомцем
Модуль 5. Цифровая экономика и потребительские риски (4 часа)					
6	Тема 6. Как совершать покупки в Интернете	4	2	2	Практикум: оценка надёжности интернет-магазина, распознавание рекламы и баннеров
Модуль 6. Персональные данные (8 часов)					
7	Тема 7. Что такое персональные данные	4	2	2	Задание «Опасные и безопасные публикации», тест на знание видов персональных данных
8	Тема 8. Какие следы мы оставляем в Интернете	4	2	2	Практическая работа: настройки приватности в соцсети (учебный тренажёр), создание QR-кода
Модуль 7. Цифровое будущее (3 часа)					
9	Тема 9. Урок в школе будущего	3	1	2	Мини-проект «Школа моей мечты» (презентация, коллаж или макет), защита проекта. Промежуточная аттестация: защита портфолио лучших работ; итоговый тест на знание
Итого за год			**34**	**17**	**17**

Содержание учебного плана (34 часа)

Модуль 1. Цифровой мир и интернет-зависимость

Тема 1. Зачем нам нужен Интернет (3 часа)

Теория (2 часа)

- История создания Интернета: Тим Бернерс Ли, Всемирная паути
- Новые возможности Интернета: образование, общение, творчест
- Типы интернет-пользователей (на примере сквозных персонаже Рита Картинкина, Игорь Неюзеров).
- Понятие интернет-зависимости: признаки, последствия.
- Понятие сбалансированного распорядка дня.

Практика (1 час)

- Дискуссия «Как Интернет помогает мне и моим друзьям?».
- Заполнение «Дневника времени в Интернете» (фиксация времен деятельности в течение недели).
- Составление индивидуального графика «Мой сбалансированный офлайн).

Формы текущего контроля

- Устный опрос: назвать создателя WWW, перечислить типы пол
- Анализ заполненного дневника времени — выявление признако зависимости.
- Самооценка по чек-листу «Здоровая цифровая привычка».

Модуль 2. Техносфера и технические риски

Тема 2. Как устроен Интернет (4 часа)

Теория (2 часа)

- Компьютерные программы: первая в мире программа, браузер, обеспечение (софт).
- Понятие техносферы, виды цифровых устройств.
- «Три кита Интернета»: железо, софт, сети.
- Компьютерные вирусы: что это, как проникают, чем опасны.
- Правила защиты цифрового устройства от вирусов.

- Решение ситуационной задачи: «На компьютер пришло письмо неизвестного отправителя — ваши действия?».

Модуль 3. Информация и контентные риски

Тема 3. Какая бывает информация (4 часа)

Теория (2 часа)

- Что такое информация. Цифровая информация, контент.
- Ценность информации (полезная, бесполезная, вредная).
- Каналы восприятия информации (зрение, слух, осязание) и их ис Интернете.
- Единицы измерения цифровой информации (бит, байт, Кбайт и
- Формы представления информации в Интернете (текст, изображ

Практика (2 часа)

- Упражнение «Сортировка контента»: определить тип информац восприятия.
- Вычисление объёма информации: перевести 5 Мбайт в Кбайты, с калькулятором).
- Групповая работа: подготовить небольшое сообщение (тема по форматах — текстовом, с картинкой, с аудио (имитация).
- Игра «Определи ценность информации» — карточки с описание

Формы текущего контроля

- Задание «Перевод единиц измерения» (3–5 примеров).
- Наблюдение за работой в группе: умение распределять роли и п результат.
- Кратковременная самостоятельная работа «Виды и формы инфо

Тема 4. Как работает поиск в Интернете (4 часа)

Теория (2 часа)

- Поиск информации. Поисковые системы (Яндекс, Google и др.).
- Полезные ресурсы (энциклопедии, образовательные сайты).
- Контентные риски: столкновение с неприятным или опасным ко (жестокость, агрессия, обман).
- Способы защиты: настройки безопасного поиска, кнопка «пожа

- Письменные ответы на вопросы: «Что делать, если увидел стра
включить безопасный поиск?».
- Взаимопроверка результатов поиска в парах.

Модуль 4. Общение и коммуникационные риски

Тема 5. Как люди общаются в Интернете (4 часа)

Теория (2 часа)

- Сервисы для общения: электронная почта, чаты, мессенджеры,
- Рэй Томлинсон — первое электронное сообщение.
- Плюсы и минусы цифрового общения (скорость, доступность vs
обмана).
- Правила онлайн-общения (нетикет): вежливость, грамотность, у
собеседнику.

Практика (2 часа)

- Ролевая игра «Диалог в чате»: смоделировать вежливый и грубы
общения, сравнить.
- Анализ ситуаций «Что делать, если незнакомец просит личные д
- Составление «Кодекса общения в классном чате» (5–7 правил).
- Упражнение на эмпатию: как понять чувства собеседника по тек
смайлы, уточняющие вопросы).

Формы текущего контроля

- Опрос по правилам нетикета (перечислить 3 основных).
- Оценка участия в ролевой игре (наблюдение учителя).
- Проверка созданного «Кодекса общения» — полнота и реалисти

Модуль 5. Цифровая экономика и потребительские риски

Тема 6. Как совершать покупки в Интернете (4 часа)

Теория (2 часа)

- Цифровая экономика: реальные и виртуальные товары.
- Первый в мире интернет-магазин.
- Критерии надёжности интернет-магазина (отзывы, контакты, сп
- Плюсы и минусы интернет-магазинов.

Формы текущего контроля

- Тест по критериям надёжного интернет-магазина.
- Проверка памятки (наличие ключевых правил: проверка SSL-се
  возврат товара).
- Решение кейса в письменной форме.

Модуль 6. Персональные данные

Тема 7. Что такое персональные данные (4 часа)

Теория (2 часа)

- Общедоступная и персональная информация.
- Персональные данные: определение, примеры.
- Виды персональных данных (по степени важности: ФИО, адрес,
  паспортные данные и др.).
- Зачем злоумышленникам персональные данные.
- Основные правила защиты персональных данных.

Практика (2 часа)

- Игра «Опасные / безопасные публикации» — разбор профилей
  персонажей (что можно публиковать, а что нельзя).
- Заполнение анкеты-тренажёра: отметить, какие поля можно зап
  профиле, а какие — только в закрытом.
- Составление мини-плаката «Мои личные данные — моя личная
- Работа в парах: обсудить ситуацию «Друг попросил пароль от а
  безопасную стратегию.

Формы текущего контроля

- Тест на различение видов персональных данных (5 вопросов).
- Анализ созданного плаката — понимание рисков.
- Письменный ответ: «Какие три вопроса незнакомец не должен з
  интернете?».

Тема 8. Какие следы мы оставляем в Интернете (4 часа)

Теория (2 часа)

- Понятие цифрового следа (информация, остающаяся после посе
  публикаций, лайков).

- Создание QR-кода (в онлайн-генераторе) с закодированной поле (например, правилом безопасности).
- Упражнение «Удали след»: что делать, если по ошибке опублик

Формы текущего контроля

- Письменные ответы: «Приведите 3 примера цифровых следов».
- Практическое задание: настроить приватность по инструкции (н
- Проверка созданного QR-кода (работоспособность, безопасност

Модуль 7. Цифровое будущее

Тема 9. Урок в школе будущего (3 часа)

Теория (1 час)

- Какие цифровые технологии уже меняют образование (интеракт облачные дневники, онлайн-курсы).
- Элементы школы будущего: дополненная реальность на уроках, экскурсии, робототехника.
- Разговор о профессиях будущего (в общем виде).

Практика (2 часа)

- Мозговой штурм «Каким будет урок через 20 лет?».
- Мини-проект: «Школа моей мечты» (индивидуально или в пара виде рисунка, коллажа, слайд-презентации или макета.
- Защита проектов перед группой (по 2–3 минуты на выступлени
- Общая дискуссия: «Как цифровые технологии помогают учитьс оставить без технологий?».

Формы текущего контроля

- Оценка проекта по критериям (оригинальность, отражение цифр качество представления).
- Устные ответы и активность в дискуссии.
- Самооценка участника: что нового узнал о цифровом будущем.

1.5. Система контроля и формы аттестации

Система контроля

2. Промежуточная аттестация (по завершении учебного года)

- Портфолио лучших работ — отбор наиболее удачных практичес памяток, проектов за год. Защита портфолио (краткая презентац
- Итоговый тест из 20 вопросов, охватывающий все 7 модулей (зн правил безопасности, терминов).
- Комплексное практическое задание — например, провести оцен вымышленного аккаунта, найти недостоверную новость, предло действий в нестандартной ситуации.

3. Функции контроля

Контроль служит инструментом для подтверждения обучающи результатов (предметных, метапредметных, личностных). Ре фиксируются в оценочных листах, используются для корректиров траекторий обучения и определения уровня сформирова компетентности к концу курса.

Виды контроля и аттестации

Вид	Сроки	Цель	
Входная диагностика	Сентябрь	Определить стартовый уровень знаний и умений обучающихся	Тест (5– «Я в Ин
Текущий контроль	Постоянно (на каждом занятии)	Отслеживание усвоения материала, корректировка образовательного процесса	Устный работа, тест, ке
Промежуточна я аттестация	Февраль–апрель (в зависимости от класса)	Оценка результатов за полугодие / после крупного модуля	Проект, круглый задание
Итоговая аттестация	Май	Подтверждение планируемых результатов за учебный год	Итогов портфол шаги»

Критерии оценки для итоговой аттестации

Оценочные материалы (общая характеристика)

Оценочные материалы служат инструментом для:

- определения уровня сформированности цифровой компетентнос
- выявления достижения планируемых результатов по каждому м год;
- корректировки образовательного процесса и индивидуальных тр

Принципы разработки:

- Валидность — задания проверяют именно те компетенции, кото программе (например, тест на виды рисков не включает посторо
- Надёжность — при повторном применении в сходных условиях стабильны (используются стандартизированные шкалы, чёткие
- Объективность — оценка исключает субъективизм за счёт испо эталонов ответов, критериальных рубрик и экспертных карт.

Возрастная адаптация: для 10–11 лет используются игровые и нагля с персонажами, тесты с картинками).

Диагностические методики и задания по группам результатов

Предметные результаты (знания и практические умения)

Формы контроля:

- Терминологические диктанты / тесты закрытого и открытого ти понятий: интернет-зависимость, фишинг, кибербуллинг, персон код и др.).
- Решение типовых кейсов (ситуационные задачи, где нужно выб алгоритм действий).
- Практические задания на цифровых тренажёрах (настройка при безопасного поиска, распознавание фейков).
- Итоговый тест (20 вопросов, охватывающих все 7 модулей).

Примеры заданий:

Пример 1. Тестовое задание (предметное знание): Выбери правиль персональные данные? а) Любая информация о человеке в Интерн фамилия; в) Информация, позволяющая идентифицировать ко

Средний	50–84%	Допускает отдельные ошибки, усвоены.
Низкий	менее 50%	Не различает виды рисков, не правилами.

Для практических заданий — чек-лист выполнения (каждый шаг ал

Метапредметные результаты

Формы контроля:

- Наблюдение с заполнением экспертной карты — на групповых играх, общих обсуждениях (например, при разыгрывании диало решении кейса «Что делать с незнакомцем?»). Педагог фиксиру друг друга, предлагать идеи, соблюдать очерёдность высказыва
- Рефлексивные листы и «Дневник времени в Интернете» — обуч оценивают, сколько времени они проводят в Сети, какие сайты соблюдают ли правила безопасности. Дневник может быть в вид со смайликами (например, «сегодня я не переходил по подозрит »).
- Игровые задания на критическое мышление — сравнить две кар коротких текста (например, рекламу и реальный отзыв), найти я фейк, выбрать правильный вариант. Задания выполняются в пар коллективным обсуждением.
- Коллективные мини-проекты (например, создание плаката «Пра Интернете» или памятки «Как не попасться на удочку мошенни умение распределить роли (кто рисует, кто пишет, кто представ и представить результат перед классом.

Пример задания: «Как распознать опасную ссылку или сооб (демонстрируется на экране или раздаётся на карточках): тебе пр игрового друга: «Привет! Заходи на этот сайт, там дают бесплатн любимой игры: http://skiny-besplatno.ru». Рядом — ещё од одноклассника в общем чате: «Ребята, вот ссылка на викторину по которую мы сегодня проходили: http://bezopasnost-school.ru». Зада 5–7 минут): 1. Обсудите с соседом/соседкой: какая из двух с опасной? Почему? 2. Запишите (или нарисуйте в тетради) два

	щедрое обещание», «нет проверки от взрослых»)		
Сотрудничество в паре	Оба активно обсуждают, слушают друг друга, приходят к общему решению	Говорит в основном один, другой соглашается без обсуждения	
Способность к простой рефлексии	По окончании пары говорит, что было легко/трудно, называет одно новое знание	Отвечает односложно («всё хорошо»)	

Итоговая оценка: 8–9 баллов — высокий уровень метапредметных
— средний уровень; 3–4 балла — низкий уровень (требует
внимание). Результаты фиксируются в листе наблюдений и
корректировки работы в группах (например, более слабые пары по
варианты с подсказками).

Критерии оценки личностных результатов (качественный анализ, бе

Показатель	Проявляется устойчиво (✔)	Проявляется ситуативно (◐)	
Ответственное отношение к публикации личной информации	Самостоятельно не публикует лишнее (адрес, телефон), спрашивает разрешения у родителей	Иногда публикует, но после напоминания учителя или родителей исправляет ошибку	
Нетерпимость к кибербуллингу (обидам в Интернете)	В обсуждении кейсов предлагает защитить того, кого обижают; говорит, что нужно сообщить взрослым	Не обижает сам, но и не вмешивается, когда обижают других	
Мотивация к саморазвитию в цифровой сфере	Задаёт вопросы на уроках, предлагает свои примеры, с радостью участвует в проектах	Выполняет задания, но без лишней инициативы (делает только то, что просят)	

Важно: результаты личностного развития не переводятся в о
фиксируются в характеристике обучающегося, в портфолио,
индивидуальных бесед с ребёнком и родителями, а также для поощ
ответственное поведение в Интернете», наклейки «Знаток безопасн

Комплект диагностических материалов с игровыми и наглядными

Проектное задание (групповое — плакат или памятка)	Интегральная оценка предметных, метапредметных и личностных результатов	Апрель	Тема: «Правил Интернете» (р
Итоговая аттестация (тест из 15 вопросов + защита портфолио + простой кейс)	Подтверждение планируемых результатов за учебный год	Май	Портфолио пр минуты), кейс

Критерии оценки проектного задания

Тема проекта (групповой, 3–4 человека): «Плакат "Безопасный
А3).

Критерий	Макс. балл	Описан
Предметная полнота	5	На плакате есть не менее 3 пр модулей (например: «Не сооб отвечай незнакомцам», «Спра
Практическая применимость	4	Правила понятны пятиклассн выполнять в реальной жизни.
Креативность и оформление	3	Есть рисунки, яркие цвета, кр текст, плакат привлекает вни
Метапредметные навыки (работа в группе)	4	Все участники что-то делали пишет, третий рассказывает), дружно.
Личностная позиция	4	На плакате есть призыв помо «Если кто-то обижает — скаж забота о своих данных.
Итого	20	Высокий: 17–20 баллов (отли командная работа); Средний: правила, но не все понятны и трудом); Низкий: 0–10 баллов соответствует теме или сдела остальные не участвовали).

Обеспечение объективности и надёжности

- Стандартные ключи — для тестов созданы простые листы ответ

личностное развитие фиксируется без травмирующих баллов, формате.

Раздел 2. Рабочая программа воспитания

2.1. Цель, задачи и целевые ориентиры воспитания

Цель воспитания

Формирование у обучающихся ответственного, осознанного и безо цифровой среде, развитие ценностного отношения к личной инфо культурному наследию и другим пользователям Интернета, а активной гражданской позиции в вопросах противодейств мошенничеству и распространению недостоверной информации.

Задачи воспитания

Направление воспитания	Задачи
Гражданско-патриотическое	— Воспитывать уважение к законодательству Р информационной безопасности, авторского пра персональных данных. — Формировать активную позицию по противо экстремизму и противоправному контенту в Ин
Духовно-нравственное	— Воспитывать доброжелательное отношение пользователям, нетерпимость к кибербуллингу форме агрессии в Сети. — Формировать навыки этичного и уважитель онлайн-среде (нетикет).
Интеллектуальное (информационное)	— Развивать критическое мышление, способно достоверную информацию от фейков. — Формировать ответственное отношение к ра информации (репосты, комментарии).
Формирование культуры здоровья	— Формировать навыки сбалансированного ис цифровых устройств, профилактика интернет-з цифрового утомления. — Воспитывать осознанное отношение к лично здоровью при работе в Интернете.

	пароли, не публикует лишнюю информаци достоверность данных.
Этичный коммуникатор	Соблюдает правила нетикета, не участвует поддерживает жертв кибербуллинга, умеет разрешать конфликты онлайн.
Критически мыслящий гражданин	Отличает фейки от правды, проверяет инфо распространяет недостоверные новости, ув право.
Цифровой здоровьесберегатель	Контролирует время в Интернете, соблюда онлайн/офлайн, знает признаки интернет-за им противостоять.
Активный созидатель	Участвует в создании позитивного контент и сверстникам в вопросах кибербезопаснос к IT-профессиям.

2.2. Формы и методы воспитания

Формы воспитательной работы

Форма	Пример использования в курсе «Киб
Этическая беседа	Обсуждение ситуаций из жизни: «Как посту попросил пароль?», «Почему нельзя смеятьс кибербуллинга?».
Диспут / дискуссия	«Стоит ли публиковать всё в соцсетях?», «К ответственность за фейковую новость?».
Ролевая игра	Разыгрывание диалога с незнакомцем в чате ситуации кибербуллинга и поиск выхода.
Кейс-метод	Разбор проблемных воспитательных ситуаци комментариях — твои действия?».
Коллективное творческое дело (КТД)	Совместное создание плаката «Безопасный I видеоролика или социальной рекламы.
Проектная деятельность	Создание памятки для младших школьников для классного чата.
Акция / флешмоб	Школьная акция «День безопасного Интерне рисунков «Что такое кибербуллинг?»

сознания	пример, этическая беседа, диспут	размещения л примеры из ре кибермошенн
Методы организации деятельности	Приучение, педагогическое требование, создание воспитывающих ситуаций, поручение	Ежедневное за времени в Инт правил работы
Методы стимулирования	Поощрение, соревнование, похвала, награждение	Грамоты «Зна кибербезопасн лучшую памят
Методы контроля и самопознания	Наблюдение, рефлексия, самооценка, анкетирование	Заполнение ре самооценка ци анализ дневни
Воспитательные технологии	Кейс-технология, игровые технологии, проектная технология, технология КТД	Разбор ситуац создание груп проведение кв

2.3. Условия организации воспитания

Воспитывающая среда

- Учебный кабинет — оборудован для групповой работы, проведе просмотра учебных видеоматериалов по кибербезопасности.
- Цифровая среда — использование безопасных образовательных демонстрация позитивных примеров цифрового поведения.
- Пространство самовыражения — стенд «Безопасный Интернет» творческих работ обучающихся (плакаты, памятки, комиксы).

Педагогические условия

- Личный пример педагога в соблюдении правил цифровой гигие
- Создание ситуаций успеха и поддержки для каждого обучающе
- Индивидуальный подход при работе с детьми, испытывающими социальной адаптации.
- Привлечение родителей к обсуждению вопросов кибербезопасн собрания, совместные проекты).

2.4. Календарный план воспитательной работы

Календарный план составлен на 2025–2026 учебный год. Мероп
модулям программы, федеральным и региональным памятны
безопасности и цифровой культуры.

№	Дата (ориентир)	Название мероприятия / дела	Форма проведения	Участники	Направление воспитания	Модуль связи
1	Сентябрь	«Вводный урок: Я — пользователь Интернета»	Этическая беседа + анкетирование	Вся группа	Информационное, формирование культуры здоровья	Модуль 1
2	Сентябрь	Акция «Неделя безопасного Рунета» (в рамках всероссийской акции)	Игра-квест, просмотр видео, обсуждение	Вся группа	Гражданско-патриотическое, информационное	Модули 1–2
3	Октябрь	«Кто такой этичный пользователь?»	Этическая беседа + работа в парах	Вся группа	Духовно-нравственное, информационное	Модуль 4
4	Октябрь	Конкурс на лучшую памятку «Мои правила безопасности в Интернете»	Творческий конкурс	Индивидуально	Формирование культуры здоровья, информационное	Модули 2–3
5	Ноябрь	«Персональные данные — моя личная граница»	Ролевая игра + создание плаката	Групповая работа (3–4 чел.)	Духовно-нравственное, правовое	Модуль 6
6	Декабрь	«Что делать, если обижают в Интернете?» (приурочено к Международному дню борьбы с буллингом)	Кейс-метод + дискуссия	Вся группа	Духовно-нравственное, сплочение коллектива	Модуль 4
7	Декабрь	Мастерская «Создаём социальную рекламу о кибербезопасности»	Коллективное творческое дело (КТД)	Групповая работа (5–6 чел.)	Гражданско-патриотическое, творческое	Модули 4–7
8	Январь	Встреча с IT-специалистом (приглашённый гость)	Встреча с интересными людьми	Вся группа	Профессиональное самоопределение, интеллектуальное	Модуль 7
9	Февраль	«Кибербезопасность в семье» (приурочено к Международному дню безопасного Интернета)	Родительское собрание + совместный проект «Безопасный Интернет для всей семьи»	Обучающиеся + родители	Все направления	Все модули
10	Февраль	Конкурс рисунков и плакатов «Безопасный Интернет глазами детей»	Выставка + конкурс	Индивидуально + группа	Духовно-нравственное, творческое	Модули 1–6
11	Март	«Фейки вокруг нас: как не дать себя обмануть»	Диспут + практикум по фактчекингу	Вся группа	Интеллектуальное (информационное), гражданское	Модуль 3
12	Апрель	Проект «Школа будущего: Интернет без	Проектная	Групповая	Профессиональное,	Модуль 7

		опасностей»	деятельность	работа (3–4 чел.)	творческое, сплочение коллектива	
13	Апрель	Турнир знатоков кибербезопасности (в рамках недели безопасности)	Командная игра-викторина	Группы (команды по 5 чел.)	Интеллектуальное, сплочение коллектива	Все модули
14	Май	Итоговое занятие «Я — ответственный пользователь»	Защита портфолио + рефлексивный круг	Вся группа	Все направления воспитания	Все модули

Примечание к календарному плану:

- План является примерным и может корректироваться с учётом р расписания, возможностей школы и запросов обучающихся (при
- Даты мероприятий привязаны к учебным периодам (окончание н даты) — принцип актуальности.
- Мероприятия отражают специфику предметного содержания (ки — принцип конкретики.

2.5. Результативно-диагностическая часть (ожидаемые резул воспитания)

Результаты воспитательной деятельности оцениваются качеств баллов) через:

Метод диагностики	Что оценивается
Наблюдение педагога (с заполнением карты)	Проявление ответственности, этичности, помощи другим, активности в обсуждениях
Анкетирование обучающихся	Отношение к правилам безопасности, мотивация, самооценка цифровых привычек
Анализ продуктов деятельности (портфолио, плакаты, проекты)	Отражение ценностных установок (нетерпимость к агрессии, ответственность за репутацию)
Рефлексивные листы и дневники	Осознание собственного поведения в Интернете, готовность к самоизменению
Отзывы родителей и педагогов школы	Перенос навыков безопасного поведения в реальную жизнь

Ежегодный анализ результатов воспитания фиксируется в дополнительного образования и используется для корректиро работы на следующий учебный год.

2.6. Связь рабочей программы воспитания с программой кур

Календарный план воспитательной работы логически встроен в м программы:

Модуль 5. Цифровая экономика и потребительские риски	Конкурс плакатов, турнир знатоков
Модуль 6. Персональные данные	Ролевая игра «Мои персональные д граница»
Модуль 7. Цифровое будущее	Проект «Школа будущего», встреча

Таким образом, рабочая программа воспитания обеспечивает не обучения и воспитания в процессе освоения курса «Кибербезопас формированию не только цифровых компетенций, но и ответс социально активной личности обучающегося.

Раздел 3. Комплекс организационно-педагогических

3.1. Календарный учебный график

Календарный учебный график является обязательной часть педагогических условий и определяет временные рамки реализации

Общие параметры учебного года

Параметр	Значение
Срок реализации программы	1 год
Продолжительность учебного года	34 учебные недели (для каждого
Начало учебного года	1 сентября текущего года
Окончание учебного года	31 мая текущего учебного года
Количество учебных дней в году	170 дней (34 недели × 5 дней)
Количество учебных часов в год	34 часа (1 час в неделю)
Продолжительность занятия	45 минут (1 академический час)
Периодичность занятий	1 раз в неделю
Режим занятий	Расписание утверждается дирек ежегодно

Календарный учебный график (на одну группу)

декабря	занятий)	
27 декабря – 11 января	2 недели	Зимние каникулы (занятия не проводятся)
12 января – 6 марта	8 недель (8 занятий)	Реализация модулей 5–6 (темы 6–8)
7 марта – 15 марта	1 неделя	Дополнительные каникулы для 5 классов (занятия не проводятся)
16 марта – 30 апреля	7 недель (7 занятий)	Реализация модуля 7 (тема 9). Подготовка и защита проекта «Школа будущего»
1 мая – 10 мая	1 неделя	Весенние каникулы (майские праздники)
11 мая – 30 мая	3 недели (3 занятия)	Повторение и обобщение. Итоговая аттестация

График проведения аттестационных процедур

№ п/п	Вид аттестации	Сроки	Форма
1	Входная диагностика	1–2 неделя сентября	Тест + анкета
2	Текущий контроль	В течение всего периода	Устный опрос, практиче работы, мини-тесты, кей
3	Промежуточная аттестация (полугодие)	Апрель (после модуля 7)	Защита проекта «Школа будущего»
4	Итоговая аттестация	20–30 мая	Итоговый тест + защита портфолио «Мои безопасные шаги»

3.2. Условия реализации программы

Материально-техническое обеспечение

№	Наименование

9	Печатные учебные материалы
10	Доска интерактивная

Кадровое обеспечение

Требование	Характеристика
Педагогическая должность	Педагог дополнительного образования
Квалификация	Высшее или среднее профессиональное образо соответствующей профилю программы (инфор психология)
Профессиональные компетенции	Владение основами кибербезопасности, знание психологии, умение применять активные метод использования цифровых образовательных рес
Повышение квалификации	Прохождение курсов повышения квалификаци области цифровой грамотности и кибербезопас в 3 года)

Информационное обеспечение (интернет-ресурсы)

1. Дети России онлайн — портал проектов Фонда Развития Интерне http://detionline.com

2. Образовательный портал для родителей от Лаборатории Касперс https://kids.kaspersky.ru

3. Электронные версии журнала «Дети в информационном обществ http://detionline.com/journal/numbers

3.3. Методическое обеспечение

Учебно-методическое обеспечение

№	Вид обеспечения	Наименование
1	Основная литература	Солдатова Г.У., Чигарькова С.В., Пермякова И.Д «Кибербезопасность» 5–9 классы. — М.: Русское
2	Учебники	Солдатова Г.У., Чигарькова С.В., Пермякова И.Д учебник для 5 класса. — М.: Русское слово (и ана

Перечень методических разработок для педагога

№	Название	Формат	
1	Сценарии занятий по всем темам 5–9 классов	Текстовый документ	Проведение времени, ф для обсужд
2	Карточки с ситуационными кейсами (3–4 варианта на каждую тему)	Раздаточный материал	Организаци работы по р ситуаций
3	Чек-листы и памятки для практических работ	Раздаточный материал	Помощь об выполнени «Как оцени
4	Оценочные листы (экспертные карты)	Шаблоны для заполнения	Фиксация р за метапред личностны
5	Презентации к каждому занятию (PowerPoint)	Электронный файл	Визуальное лекционной примеров
6	Инструкции по работе с цифровыми тренажёрами и онлайн-ресурсами	Текстовый документ	Организаци с устройств
7	Шаблоны портфолио и рефлексивных листов	Раздаточный материал	Фиксация л самооценки

Рекомендации по организации образовательного процесса

4. Использование активных методов обучения: приоритет отдаётся заданиям, работе в парах и группах, дискуссиям, а не пассивному п лекций.

5. Индивидуализация обучения: для детей с разным уровнем подгот предусмотрены разноуровневые задания (базовые — для всех, повы — для мотивированных).

6. Здоровьесбережение: каждые 10–15 минут смена вида деятельнос физкультминутки; контроль времени работы за экраном; обсуждени утомления.

7. Безопасность при работе в Интернете: все онлайн-занятия провод включёнными фильтрами контента; используются учебные тренажё

11. Солдатова Г.У., Чигарькова С.В., Илюхина С.Н. Социокультурн
в молодёжной среде. Мы в ответе за цифровой мир: учебное пособи
Центр, 2021.

3.5. Список литературы для обучающихся

12. Солдатова Г.У., Чигарькова С.В., Пермякова И.Д. Кибербезопас
5 класса. — М.: Русское слово.

13. Электронные версии журнала «Дети в информационном общест
обучающихся). — URL: http://detionline.com/journal/numbers

3.6. Нормативная база

Перечень нормативно-правовых документов для проектирова
дополнительной общеобразовательной программы:

14. Федеральный Закон от 29.12.2012 № 273-ФЗ «Об образовании в
Федерации» (в ред. от 15.10.2025).

15. Федеральный государственный образовательный стандарт осно
образования (утв. приказом Минпросвещения РФ от 31.05.2021 № 2

16. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных д

17. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от
причиняющей вред их здоровью и развитию».

18. Указ Президента Российской Федерации от 07.05.2024 № 309 «О
целях развития РФ на период до 2030 года и на перспективу до 203

19. Указ Президента Российской Федерации от 09.11.2022 № 809 «О
Основ государственной политики по сохранению и укреплению тра
российских духовно-нравственных ценностей».

20. Концепция развития дополнительного образования детей до 203
распоряжением Правительства Российской Федерации от 31.03.202
01.07.2025).

21. Концепция развития детско-юношеского спорта в Российской Ф
года (утв. распоряжением Правительства Российской Федерации от
р) (в ред. от 20.03.2023).

22. Паспорт национального проекта «Молодежь и дети».

26. Приказ Министерства образования и науки Российской Федера
просвещения Российской Федерации от 05.08.2020 г. № 882/391 «О
осуществлении образовательной деятельности по сетевой форме ре
образовательных программ».

27. Приказ Министерства просвещения Российской Федерации от 2
«Об утверждении Порядка организации и осуществления образоват
деятельности по дополнительным общеобразовательным программа

28. Приказ Министерства труда и социальной защиты Российской Ф
22.09.2021 № 652н «Об утверждении профессионального стандарта
дополнительного образования детей и взрослых"».

Приложения

Приложение 1. Календарный учебный график на 2025–2026 у

№ занятия	Дата (план)	Тема занятия	Кол-во часов	Форма занятия	Форма контроля	Модуль
1	1–5 сентября	Входная диагностика. Знакомство с курсом	1	Беседа + тестирование	Входной тест, анкета	Вводное
2	8–12 сентября	Создание Интернета. Тим Бернерс Ли	1	Лекция с презентацией	Устный опрос	Модуль 1
3	15–19 сентября	Типы интернет-пользователей	1	Работа в парах	Наблюдение, взаимооценка	Модуль 1
4	22–26 сентября	Интернет-зависимость. Сбалансированный распорядок дня	1	Практикум + дневник	Дневник времени	Модуль 1
5	29 сентября – 3 октября	Компьютерные программы. Браузер. Софт	1	Лекция	Терминологический диктант	Модуль 2
6	6–10 октября	«Три кита Интернета»: железо, софт, сети	1	Работа в парах	Практическое задание	Модуль 2
7	13–17 октября	Компьютерные вирусы: как проникают и чем опасны	1	Кейс-метод	Решение кейса	Модуль 2
8	20–24 октября	Правила защиты от вирусов. Создание памятки	1	Практическая работа	Проверка памятки	Модуль 2
9	10–14 ноября	Что такое информация. Цифровая информация	1	Лекция + игра	Устный опрос	Модуль 3
10	17–21 ноября	Единицы измерения информации	1	Практикум с калькулятором	Вычисление объёма данных	Модуль 3
11	24–28 ноября	Формы представления информации	1	Групповая работа	Заполнение таблицы	Модуль 3
12	1–5 декабря	Поисковые системы. Как работает поиск	1	Лекция + демонстрация	Поисковое задание	Модуль 3
13	8–12 декабря	Контентные риски. Неприятный контент	1	Кейс-метод	Анализ ситуаций	Модуль 3
14	15–19 декабря	Безопасный поиск. Кнопка «пожаловаться»	1	Практическая работа	Настройка фильтров	Модуль 3
15	22–26 декабря	Сервисы для общения. Правила нетикета	1	Ролевая игра	Наблюдение	Модуль 4
16	12–16 января	Плюсы и минусы цифрового общения	1	Дискуссия	Активность в дискуссии	Модуль 4
17	19–23 января	Общение с незнакомцами в Интернете	1	Кейс + работа в парах	Решение кейса	Модуль 4
18	26–30 января	Цифровая экономика. Интернет-магазины	1	Лекция	Устный опрос	Модуль 5
19	2–6 февраля	Критерии надёжного интернет-магазина	1	Практикум	Чек-лист оценки	Модуль 5

20	9–13 февраля	Баннеры, реклама. Мошенничество	1	Кейс-метод	Распознавание обмана	Модуль 5
21	16–20 февраля	Что такое персональные данные. Виды ПД	1	Лекция + игра «Опасные публикации»	Тест	Модуль 6
22	26 февраля – 2 марта	Как защитить персональные данные	1	Практическая работа	Создание плаката	Модуль 6
23	3–6 марта	Цифровой след: что остаётся в Интернете	1	Беседа + поиск следов	Письменный ответ	Модуль 6
24	16–20 марта	Понятие приватности. Настройки приватности	1	Практическая работа (симулятор)	Настройка профиля	Модуль 6
25	23–27 марта	QR-код: что это и как безопасно использовать	1	Практическая работа	Создание QR-кода	Модуль 6
26	30 марта – 3 апреля	Повторение модуля 6. Промежуточная проверка	1	Тестирование	Промежуточный тест	Модуль 6
27	6–10 апреля	Цифровые технологии в образовании	1	Лекция + обсуждение	Устный опрос	Модуль 7
28	13–17 апреля	Проект «Школа будущего» — подготовка	1	Групповая работа	Наблюдение	Модуль 7
29	20–24 апреля	Проект «Школа будущего» — защита	1	Защита проектов	Оценка проекта	Модуль 7
30	27–30 апреля	Повторение. Подготовка к итоговой аттестации	1	Игра-викторина	Активность	Все модули
31	11–15 мая	Итоговый тест	1	Индивидуальная работа	Тест (15 вопросов)	Итоговая аттестация
32	18–22 мая	Защита портфолио «Мои безопасные шаги»	1	Презентация портфолио	Оценка портфолио	Итоговая аттестация
33	25–29 мая	Итоговое занятие. Рефлексия «Я — ответственный пользователь»	1	Круглый стол	Самооценка	Итоговая аттестация
34	(резерв)	Резервное занятие	1	По усмотрению педагога	–	–

Условные обозначения:

- «Дневник времени» — заполнение таблицы учёта времени в Ин
- «Чек-лист» — оценочный лист с критериями.
- «Симулятор» — учебный тренажёр (не реальный сайт).

Приложение 2. Оценочные (контрольно-измерительные) ма

2.1. Входная диагностика

Инструкция: «Прочитай вопросы. Выбери правильный ответ ил
ответ».

№	Вопрос	Варианты ответов
1	Что такое Интернет?	а) Компьютерная игра б) Всемирная сеть, соединяющая компы в) Программа для рисования
2	Можно ли публиковать в соцсетях свой домашний адрес?	а) Да, всегда б) Только с разрешения родителей в) Нет, никогда
3	Что такое пароль?	а) Секретная комбинация символов для б) Имя пользователя в) Адрес сайта
4	Как ты думаешь, сколько времени в день можно проводить в Интернете школьнику?	(свободный ответ)
5	Что нужно сделать, если незнакомец просит прислать твоё фото?	а) Отправить фото б) Посоветоваться с родителями и не от в) Попросить денег за фото
6	Как часто ты советуешься с родителями по поводу того, что делаешь в Интернете?	а) Всегда б) Иногда в) Никогда

Максимальный балл: 6. Уровни: высокий — 5–6 баллов; средний -
— 0–2 балла.

2.2. Итоговый тест (15 вопросов)

Инструкция: «Внимательно прочитай каждый вопрос. Обведи

4	Какой пароль самый надёжный?	а) 123456 б) qwerty в) Kb5#Rm9!Lp2
5	Что нужно сделать, если увидел в Интернете жестокое видео?	а) Закрыть глазки б) Рассказать взрослому и нажать «по в) Отправить другу
6	Что такое фишинг?	а) Рыбалка б) Вид мошенничества — выманивани в) Компьютерная игра
7	Можно ли поставить фотографию из Интернета на свой аватар?	а) Да, любую б) Только с разрешения автора или ес в) Нет, никогда
8	Что такое «цифровой след»?	а) След от мышки б) Информация, которую ты оставляе в) Пароль
9	Как защитить свой аккаунт в соцсети? (напиши 2 способа)	(свободный ответ)
10	Что такое кибербуллинг?	а) Полезное общение б) Травля, оскорбления в Интернете в) Покупки онлайн
11	Какая ссылка может быть опасной?	а) http://school.ru б) http://skiny-besplatno-secret.ru в) http://ya.ru
12	Что означает кнопка «пожаловаться» (жалоба) на сайте?	а) Позвать друга б) Сообщить модератору о нарушени в) Поставить лайк
13	Что такое QR-код?	а) Квадратный код с информацией б) Игра в) Антивирус
14	Придумай правило безопасности при покупках в Интернете.	(свободный ответ)
15	Что делать, если ты понял, что перешёл по мошеннической ссылке? (напиши 2 действия)	(свободный ответ)

Ключи к тесту (для педагога):

№	Правильный ответ

10	б
11	б
12	б
13	а
14	Любое разумное правило (например, «Проверяй отзывы перед покупкой»)
15	2 действия: не вводить данные, сообщить взрослому, сменить пароль

Максимальный балл: 15. Уровни: высокий — 13–15 баллов; сред
низкий — 0–7 баллов.

2.3. Анкета для оценки личностных результатов «Я в Интернете»

Инструкция: «Отметь один ответ, который больше всего тебе
выбрать ☺ (да), □ (иногда) или ☹ (нет)».

№	Утверждение	Да (☺)
1	Я всегда спрашиваю разрешения у родителей, прежде чем скачать игру или приложение.	
2	Когда я вижу, что кого-то обижают в чате или игре, я говорю об этом взрослому.	
3	Я не пишу в Интернете свой адрес и телефон без разрешения родителей.	
4	Мне интересно узнавать новое о том, как защитить себя в Интернете.	
5	Я могу отказать другу, если он просит мой пароль от аккаунта.	
6	Перед тем как поставить чужое фото на аватар, я проверяю, можно ли это делать.	
7	Я стараюсь не сидеть в Интернете дольше, чем планировал(а).	

Обработка (для педагога): каждый ответ ☺ — 2 балла, □ — 1 б
Суммарно: 12–14 баллов — высокий уровень личностной зр
кибербезопасности; 7–11 баллов — средний уровень (треб
напоминание); 0–6 баллов — низкий уровень (рекомендована инди
работа с родителями). Личностные результаты не переводятся в ф

Качество выступления	4	Обучающийся говорит понят вопросы, укладывается в 2 ми
Самостоятельность	4	Проект выполнен самостоятел все участники что-то делали).
Итого	20	Высокий: 17–20 баллов; Сред Низкий: 0–10 баллов.

2.5. Карта наблюдения за метапредметными результатами (экспе

Заполняется педагогом на групповой работе (например, при создани
безопасности»).

ФИО обучающегося	Аргументация	Сотрудничество	Рефлексия	Сум бал
ФИО	3	2	3	8

Уровни: 8–9 баллов — высокий; 5–7 — средний; 3–4 — низкий (тре

Приложение 3. Перечни оборудования и средств обучения, д материалов

3.1. Оборудование и технические средства

№	Наименование	Количество	
1	Компьютер педагога (ноутбук) с ОС Windows/MacOS	1	С вых
2	Мультимедийный проектор или интерактивная панель	1	Для д презе
3	Экран (или белая стена)	1	–
4	Ноутбуки или планшеты для обучающихся	10–15	Из ра 1–2 че
5	Колонки (акустическая система)	1	Для п
6	Принтер чёрно-белый / цветной	1	Для п матер
7	Доска меловая или маркерная	1	Для за

4	Генератор QR-кодов (любой онлайн-сервис)	Бесплатный	Со обу
5	Антивирус (демо-версия)	Демо / бесплатная	Де ант

3.3. Дидактические материалы (раздаточные)

№	Наименование	Формат	
1	Карточки с кейсами (по темам)	Печатные, ламинированные	
2	Чек-лист «Как оценить надёжность интернет-магазина»	Печатный	
3	Бланк «Дневник времени в Интернете»	Печатный	
4	Шаблон портфолио «Мои безопасные шаги»	Печатный	
5	Плакаты-памятки (готовые)	Печатные, настенные	
6	Стикеры и наклейки «Знаток безопасности»	Печатные	
7	Карточки с QR-кодами (ссылки на полезные ресурсы)	Печатные	
8	Бланки анкет и тестов (входных, итоговых)	Печатные	

3.4. Учебно-методическая литература (на группу)

№	Наименование	Коли
1	Солдатова Г.У., Чигарькова С.В., Пермякова И.Д. Кибербезопасность. Учебник для 5 класса	10–15
2	Методическое пособие для педагога	1
3	Программа курса «Кибербезопасность» (печатная или электронная)	1

Настоящее приложение является неотъемлемой частью общеобразовательной программы «Кибербезопасность» и содерж материалы для её полноценной реализации в 5 классе. Для 6–9 разрабатываются аналогично, с усложнением содержания т