Министерство образования и науки Хабаровского края
Краевое государственное автономное нетиповое
Общебразовательное учреждение
«Краевой центр образования»

РАССМОТРЕНО
на заседании
Педагогического совета
КГАНОУ КЦО
Протокол №2
от «21» ноября 2025г.

УТВЕРЖДАЮ
Генеральный директор
КГАНОУ КЦО
_____/Черёмухин П.С.
от «21» ноября 2025г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА ТЕХНИЧЕСКОЙ НАПРАВЛЕННОСТИ

«Кибербезопасность»

Уровень освоения: стартовый
Возраст учащихся: 10-12 лет
Общий объем программы в часах: 16 часов

Составитель программы:
Валетова М.А., методист

г. Хабаровск,
2025 г.

Раздел 1. Комплекс основных характеристик ДООП

1.1. Пояснительная записка

Дополнительная общеобразовательная общеразвивающая программа «Кибербезопасность» имеет техническую направленность (IT – технологии), стартовый уровень.

Программа разработана с учетом следующих нормативно-правовых документов:

- Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»;
- Распоряжение Правительства Российской Федерации от 31 марта 2022 года № 678-р «Концепция развития дополнительного образования детей до 2030 года»;
- Приказ Минпросвещения Российской Федерации от 27 июля 2022 года № 629 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
- Постановление Главного государственного санитарного врача Российской Федерации от 28 сентября 2020 года № 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организации воспитания и обучения, отдыха и оздоровления детей и молодежи» в редакции от 01.03.2025 г.;
- Постановление Главного государственного санитарного врача Российской Федерации от 28 января 2021 года № 2 «Об утверждении санитарных правил и норм СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания»;
- Распоряжение Министерства образования и науки Хабаровского края от 26 сентября 2019 года № 1321 «Об утверждении методических рекомендаций «Правила персонифицированного финансирования дополнительного образования детей в городском округе, муниципальном районе Хабаровского края»;
- Методические рекомендациями по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы) (Письмо Министерства образования и науки Российской Федерации от 18 ноября 2015 года № 09-3242);
- Методические рекомендациями по формированию механизмов обновления содержания, методов и технологий обучения в системе дополнительного образования детей, направленных на повышение качества дополнительного образования детей, в том числе включение компонентов, обеспечивающих формирование функциональной грамотности и компетентностей, связанных с эмоциональным, физическим, интеллектуальным, духовным развитием человека, значимых для вхождения Российской Федерации в число десяти ведущих стран мира по качеству

общего образования, для реализации приоритетных направлений научно-технологического и культурного развития страны (Письмо Минпросвещения Российской Федерации от 29 сентября 2023 года № АБ-3935/06);

– Приказ краевого государственного автономного образовательного учреждения дополнительного образования «Центр развития творчества детей (региональный модельный центр дополнительного образования детей Хабаровского края)» от 27 мая 2025 года №220 П «Об утверждении Положения о дополнительной общеобразовательной общеразвивающей программе, реализуемой в Хабаровском крае»);

– Устав краевого государственного автономного нетипового образовательного учреждения «Краевой центр образования».

Актуальность программы

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

Педагогическая целесообразность

Дополнительная общеобразовательная общеразвивающая программа «Кибербезопасность» направлена на формирование у обучающихся навыков безопасного и ответственного поведения в интернет-пространстве, развитие технических и творческих способностей, а также формирование логического и критического мышления.

Обучение в программе построено на групповом взаимодействии: командные задания акцентируют сотрудничество, взаимопомощь и распределение ролей, когда вклад каждого участника важен для достижения общей цели. Становление и совершенствование компетенций происходит через вовлечение обучающихся в осмысленную индивидуальную и коллективную деятельность, что обеспечивает накопление практического опыта, осознание ценностей и формирование ответственного поведения в цифровой среде.

В результате освоения программы обучающийся приобретёт устойчивую базу знаний и практических навыков, которые позволят ему самостоятельно продолжать совершенствовать компетенции в области

информационного сбора, анализа и обработки, цифровой безопасности и этичного использования ИКТ.

Новизна программы заключается в демонстрации обучающимся всех достоинств и недостатков интернет-пространства.

Программа направлена на обучение детей ориентироваться в Информационном пространстве, проверять, оценивать получаемую информацию, защищать себя в информационном пространстве, ответственно относиться к созданию и публикации контента. Обучение по программе способствует развитию технических и творческих способностей, формированию логического мышления.

Отличительной особенностью программы является комплексный подход к формированию компетенций обучающихся. Требования к результатам подготовки охватывают не только удовлетворение познавательных интересов и умение искать дополнительную информацию, но и:

- базовые технические навыки работы с устройствами (включая персональные компьютеры) и периферийным оборудованием;
- знания основ кибербезопасности и навыки их применения в практической деятельности;
- умение организовывать и поддерживать безопасность собственного информационного пространства.

Такая совокупность результатов обеспечивает готовность обучающихся не только к техническому использованию ИКТ, но и к ответственному, безопасному и осознанному поведению в цифровой среде.

Адресат программы: Программа предназначена для группового обучения детей в возрасте 10 - 12 лет.

Форма обучения: Очная.

Объём реализации программы: 16 часов

Период	Продолжительность занятий	Кол-во занятий в неделю	Кол-во часов в неделю	Кол-во недель	Кол-во часов за период
4 мес.	1 ч.	1	1 ч.	16	16 ч.
				Итого по программе:	16 ч.

Режим организации занятий: Занятия в объединении рекомендуется проводить по 1 занятию в неделю по 1 академическому часу (45 минут).

1.2. Цель и задачи программы

Цель программы: Формирование информационной культуры и повышение уровня осведомленности учащихся в области кибербезопасности и воспитание ответственного поведения в цифровом мире.

Задачи программы:

познакомить с базовыми понятиями кибербезопасности и информационной культуры;

дать представление о типичных онлайн-рисках (фишинг, вредоносные ссылки, мошенничество, кибербуллинг).

сформировать навыки безопасного обращения с личными данными (создание и хранение паролей, настройка приватности);

научить распознавать и корректно реагировать на потенциальные угрозы в сети (подозрительные письма, фальшивые сайты, сомнительный контент).

развивать критическое мышление при оценке информации в интернете (проверка источников, распознавание фейков);

формировать умение работать с информацией: поиск, анализ, оценка достоверности и использование.

воспитывать ответственное и этичное поведение в сети (правила общения, уважение приватности других);

сформировать устойчивые установки на соблюдение цифровой гигиены и безопасных практик в повседневной деятельности.

1.3. Учебный план

№ п/п	Название темы	Количество часов			Формы аттестации/ контроля
		Всего	Теория	Практика	
1	Введение в кибербезопасность. ТБ	1	0,5	0,5	Опрос по теме
2	Личные данные: что можно и что нельзя публиковать.	1	0,5	0,5	Тестирование
3	Пароли: как придумывать и хранить.	1	0,5	0,5	Опрос по теме Выполнение практического задания. Тестирование
4	Фишинг: письма, ссылки и поддельные сайты	1	0,5	0,5	Опрос по теме Выполнение практического задания
5	Социальные сети и общение онлайн	1	0,5	0,5	Опрос по теме Выполнение практического задания
6	Безопасность фотографий и геометки	1	0,5	0,5	Опрос по теме Выполнение практического задания
7	Безопасность на мобильных устройствах	1	0,5	0,5	Опрос по теме Выполнение практического задания
8	Вредоносное ПО: вирусы, трояны, шпионское ПО	1	0,5	0,5	Опрос по теме Выполнение практического задания

9	Электронная почта: правила использования и безопасность	1	0,5	0,5	Опрос по теме Выполнение практического задания
10	Проверка информации и медиаграмотность	1	0,5	0,5	Опрос по теме Выполнение практического задания
11	Игры и внутриигровые покупки: безопасность и время	1	0,5	0,5	Опрос по теме Выполнение практического задания
12	Что делать при кибербуллинге и угрозах	1	0,5	0,5	Опрос по теме Выполнение практического задания
13	Основы авторских прав и безопасное использование контента	1	0,5	0,5	Опрос по теме Выполнение практического задания
14	Создание цифрового следа и репутация	1	0,5	0,5	Опрос по теме Выполнение практического задания
15	Основы защиты устройств: антивирусы, пароли на устройствах, шифрование	1	0,5	0,5	Опрос по теме Выполнение практического задания
16	Заключительное занятие.	1	-	1	Квест-игра
Итого:		**16**	**7,5**	**8,5**	

1.4. Содержание учебного плана

Тема 1. Введение в кибербезопасность. ТБ.

Теория: Что такое кибербезопасность, зачем она нужна, правила поведения в сети. Основные угрозы (вирусы, фишинг, мошенники, утечка личных данных). ТБ в кабинете и при работе на ПК.

Практика: Анкета о привычках в сети Интернет; разбор коротких сценариев «что правильно/что нет»; мозговой штурм «что может быть опасно в интернете».

Тема 2. Личные данные: что можно и что нельзя публиковать.

Теория: Понятие личных данных, почему их надо защищать; примеры рисков при публикации адреса, номера телефона, школы, фото.

Практика: Игра «Раздели на публичное/личное» — карточки с ситуациями; создать чек-лист, что нельзя выкладывать.

Тема 3. Пароли: как придумывать и хранить.

Теория: Принципы надёжного пароля (длина, разнообразие символов, фразы), опасности простых паролей, почему нельзя один пароль для всех сайтов.

Практика: Работа в малых группах: придумать 3 надёжных пароля по

правилам и объясняет выбор. Упражнение: превращаем фразу в пароль; обсуждение способов безопасного хранения. Мини-тест «Надежность пароля».

Тема 4. Фишинг: письма, ссылки и поддельные сайты.

Теория: Признаки фишинга (срочность, ошибки, странные ссылки, поддельный адрес отправителя).

Практика: Упражнение: «Расследование фишинговой атаки». Создать памятку «Как проверить ссылку».

Тема 5. Социальные сети и общение онлайн.

Теория: Правила общения, приватность в настройках, опасности общения с незнакомцами.

Практика: Настроить приватность на учебном (демонстрационном) аккаунте; сделать список «Правил для сообщений незнакомцам».

Тема 6. Безопасность фотографий и геометки.

Теория: Риски публикации фото (геометки, метаданные), как удалить координаты из фото.

Практика: Показать метаданные на примере; отредактировать фото (удалить геометки).

Тема 7. Безопасность на мобильных устройствах.

Теория: Значимость обновлений, контроль разрешений, установка приложений только из проверенных источников.

Практика: Проверка разрешений приложений (демонстрация); игра «Разрешать/не разрешать» с карточками.

Тема 8. Вредоносное ПО: вирусы, трояны, шпионское ПО.

Теория: Виды вредоносного ПО, как они попадают на устройство, симптомы заражения.

Практика: Кейс-разбор: что делать при подозрении на вирус; список шагов (отключить интернет, сообщить взрослым, не вводить пароли).

Тема .9. Электронная почта: правила использования и безопасность.

Теория: Безопасная работа с почтой, спам, вложения, подозрительные ссылки.

Практика: Распознать фишинговое письмо среди примеров; создать чек-лист перед открытием вложения.

Тема 10. Проверка информации и медиаграмотность.

Теория: Как отличать правду от лжи в интернете, проверка источников, базовые техники (обратный поиск изображений).

Практика: Проверить 3 новостных заголовка/картинок — правда или фейк, использовать простые инструменты проверки (поиск, сопоставление источников). Игра «Факт или вымысел».

Тема 11. Игры и внутриигровые покупки: безопасность и время.

Теория: Риски внутриигровых покупок, мошенничество, защита аккаунта (пароль, 2FA), баланс времени за экраном.

Практика: Создать правила безопасной игры и бюджета; разобрать несколько мошеннических схем в играх.

Тема 12. Что делать при кибербуллинге и угрозах.

Теория: Что такое кибербуллинг, как реагировать, кому сообщать, сохранение доказательств.

Практика: Разбор сценариев, разработка «плана действий» — скриншоты, сообщения взрослым, блокировка.

Тема 13. Основы авторских прав и безопасное использование контента.

Теория: Что такое авторское право, почему нельзя скачивать всё подряд, безопасные источники контента.

Практика: найти и указать источники для трёх изображений/мелодий; создать правила честного использования контента.

Тема 14. Создание цифрового следа и репутация.

Теория: Что такое цифровой след, как посты формируют репутацию, долгосрочные последствия.

Практика: Анализ выдуманного профиля — что можно улучшить, какие посты убрать; составить «шпаргалку» хорошего профиля.

Тема 15. Основы защиты устройств: антивирусы, пароли на устройствах, шифрование.

Теория: Защита устройства (антивирус, экран блокировки, шифрование), когда и почему применять.

Практика: Установка и запуск антивирусной проверки на учебном устройстве (демонстрация); настроить экран блокировки и PIN.

Тема 16. Заключительное занятие.

Практика: Квест-игра «БезОпасный Интернет».

Планируемые результаты

Предметные:

- Знают базовые понятия: кибербезопасность, информационная культура, персональные данные, приватность, фишинг, вредоносное ПО, кибербуллинг.
- Умеют объяснять основные виды онлайн-угроз и потенциальные последствия их применения.
- Умеют создавать и правильно хранить надёжные пароли; знают принципы двухфакторной аутентификации.
- Умеют настраивать базовые параметры приватности в популярных онлайн-сервисах (соцсети, почта, браузер) на уровне пользователя.
- Умеют распознавать фишинговые письма, подозрительные ссылки и фальшивые сайты по характерным признакам.
- Умеют применять простые средства защиты: обновление ПО, антивирусные проверки, безопасный просмотр веб-страниц.

Метапредметные:

- Умеют ясно и корректно формулировать вопросы и ответы по безопасности в сети, вести диалог о приватности и правилах поведения в онлайне.

– Планируют свои действия при возникновении онлайн-угроз (алгоритм реакции на подозрительное сообщение, обращение за помощью), оценивают риски и выбирают безопасное поведение.

– Анализируют информацию, сопоставляют источники и делают обоснованные выводы о её достоверности; распознают манипулятивные приёмы в контенте.

Личностные:

– Формируется ответственный подход к использованию цифровых технологий и уважительное отношение к приватности своей и других людей.

– Развивается этическая позиция в сети: соблюдение правил приличия, недопущение кибербуллинга, уважение авторских прав.

– Повышается готовность обращаться за помощью к взрослым/специалистам при столкновении с опасными ситуациями в сети.

Раздел 2. Комплекс организационно – педагогических условий

2.1. Календарный учебный график программы (Приложение 1)

Период обучения	Дата начала занятий	Дата окончания занятий	Кол-во учебных недель	Кол-во учебных часов	Режим занятий
4 мес.	21.01.2026 г.	23.05.2026 г.	16	16	1 раз в нед. по 1 ак. ч.

2.2. Условия реализации программы

Материально-техническое обеспечение:

– компьютеры (ноутбуки) должны быть подключены к единой сети с доступом Интернет не медленнее 10 Мбит/с;

– презентационное оборудование (проектор с экраном/телевизор с большим экраном) с возможностью подключения к компьютеру (ноутбуку) – 1 комплект;

– периферийное оборудование и оргтехника: принтер-сканер на рабочем месте педагога.

Программное обеспечение:

– операционная система – любая;

– любой современный браузер (например, Яндекс.Браузер, Chrome).

Информационное обеспечение:

– интернет-источники:

«Уроки безопасного Интернета» – Лига безопасного Интернета ссылка: https://ligainternet.ru/videouroki/,

курс «Основы интернет безопасности» ссылка: https://4brain.ru/internet_security/intro.php,

онлайн-игра по кибербезопасности ссылка: https://spoofy.ee/ru/game ;

«Урок цифры» ссылка: https://datalesson.ru/lessons.

– инструкции по настройке оборудования;

– учебная и техническая литература;

– обязательным является инструктаж по технике безопасности и беседы о здоровье сберегающем поведении в процессе работы на компьютере, интенсивной интеллектуальной деятельности.

Кадровое обеспечение: Программа реализуется педагогом дополнительного образования.

2.3. Формы аттестации

Для отслеживания результативности образовательной деятельности по программе проводятся: входной, текущий и итоговый контроль.

Входная диагностика (входной контроль) проводится с целью выявления первоначального уровня знаний, умений и возможностей обучающихся.

Формы: собеседование.

Текущий контроль осуществляется для отслеживания уровня освоения учебного материала программы и развития личностных качеств обучающихся.

Формы: анализ практической деятельности; тестирование.

Итоговый контроль проводится с целью оценки уровня и качества освоения обучающимися дополнительной общеобразовательной общеразвивающей программы (всего периода обучения по программе).

Формы: квест-игра.

2.4. Оценочный материал

Вводный контроль для определения начального уровня знаний учащихся в форме опроса (Приложение 2). Текущий контроль примеры практических заданий, тестов (Приложение 3). Итоговый контроль сценарий квест-игры (Приложение 4).

Критерии оценки качества подготовки учащегося позволяют определить уровень освоения материала, предусмотренного учебной программой. Основным критерием оценок учащегося, осваивающего программу, является грамотное и качественное выполнение практических заданий.

Критерии оценивания уровня освоения программы:

Уровень освоения	Критерии оценивания
Высокий	Предполагает: Самостоятельное и креативное выполнение заданий, полное соответствие требованиям, грамотное представление работы
Средний	Допускает: В целом успешное выполнение заданий, необходимость незначительной помощи педагога, наличие небольших недочетов в практических работах

Низкий	Допускает: Затруднения при выполнении заданий, потребность в постоянной помощи, допущение существенных ошибок, низкое качество выполнения практических работ.

2.5. Методическое обеспечение программы

Методы и приёмы организации образовательного процесса при реализации программы:

Словесные методы: объяснение, беседа, комментированное чтение, рассказ.

Практические методы: работа с текстом, составление планов, выполнение творческих заданий: составление кроссвордов, выпуск бюллетеней, листовок и чек-листов.

Игровые методы: фантазирование, живая наглядность.

Наглядные методы: показ видеоматериалов, проведение экскурсий.

Виды дидактических материалов, используемые при реализации программы:

Для обеспечения наглядности и доступности изучаемого материала педагог использует наглядные пособия следующих видов:

– схематические или символические (оформленные стенды и планшеты, таблицы, схемы, рисунки, графики, плакаты, диаграммы, чертежи, шаблоны и т.п.);

– картинные (иллюстрации, слайды, фотоматериалы и др.);

– звуковые (аудиозаписи);

– смешанные (видеозаписи, учебные кинофильмы и т.д.);

– дидактические пособия (карточки, рабочие тетради, раздаточный материал, вопросы и задания для опроса, тесты, практические задания, упражнения и др.).

– компьютерные программы в электронном виде (компьютеры с программами, CD, флеш-носители);

– учебные пособия, журналы, книги, Интернет-ресурсы.

При реализации программы с целью повышения качества и эффективности процесса обучения применяются современные эффективные технологии обучения, ориентированные не на накопление знаний, а на организацию активной деятельности обучающихся:

– компьютерные (информационные) технологии;

– технологии учебно-игровой деятельности (моделирование);

– технологии коммуникативно-диалоговой деятельности;

– квест-технологии;

– технологии личностно-ориентированного обучения; – кейс-технологии.

Информационные технологии используются в различных видах деятельности:

– при подготовке и проведении занятий;

– для создания авторских мультимедийных презентаций;

– в рамках индивидуальной и групповой деятельности;

– для самостоятельной работы;

– для накопления демонстрационных материалов к занятиям (видеоматериалы, таблицы, презентации, карты).

Алгоритм учебного занятия:

Учебное занятие по программе строится по следующему алгоритму – ход занятия:

1. Организационный момент (5 мин.);
2. Актуализация знаний (3-5 мин.);
3. Объяснение нового материала и демонстрация (10 мин.);
4. Практическое выполнение задания под руководством педагога (20 мин.);
5. Рефлексия. Подведение итогов (5 мин.).

Календарный план воспитательной работы

1.Модуль «Учебное занятие»			
№	Наименование мероприятия		Сроки, дата
1.1	Проведение тематических уроков: «Урок цифры», «Урока безопасности и навыков безопасного поведения в Интернете, информационной безопасности, повышение правовой грамотности»		В течение учебного года согласно графика
2. Модуль «Взаимодействие с родителями»			
№	Тема мероприятия	Форма организации	Сроки
3.1	Консультирование семей учащихся попавших в трудную жизненную ситуацию, а также по актуальным вопросам обучения, воспитания и личностного развития детей	Индивидуальные консультации по запросу	В течении года
3.2	Проведение мониторинга эффективности реализации проекта, с целью выявления и анализа степени удовлетворенности родителей.	Анкетирование и диагностика участников проекта	Май
3.3	Проведение родительских собраний с включением в повестку следующих вопросов: особенности ранней профориентации и предпрофессиональной подготовки учащихся, роль родителей в профориентации учащихся; организация проектной деятельности обучающихся технической направленности; участие в конкурсных мероприятиях разного уровня в рамках формирования индивидуальных образовательных траекторий учащихся.	Открытые родительские собрания	Апрель
3.4	«День открытых дверей»	Экскурсия, мастер-классы	Сентябрь
4. Модуль «Наставничество»			
№	Наименование мероприятия		Сроки, дата
4.1	Сопровождение учащихся на мероприятиях различного уровня		Согласно поступающим предложениям
5. Модуль «Профессиональное самоопределение»			
№	Наименование мероприятия		Сроки, дата
5.1	Участие в работе всероссийских профориентационных проектов, созданных в сети интернет: просмотр лекций, решение учебно-тренировочных задач, участие в мастер-классах		В течение года
5.2	Экскурсии с последующим аналитическим обсуждением IT-компаний, промышленных предприятий в г. Хабаровске		В течение года
6. Модуль «Ключевые культурно-образовательные события»			
№	Наименование мероприятия		Срок, дата
6.1	День Российской науки		08 февраля
6.2	День защитника Отечества		23 февряля
6.3	Международный женский день		08 марта

6.4	День космонавтики	Апрель
6.5	День памяти о геноциде советского народа нацистами и их пособниками в годы Великой Отечественной войны	19 апреля
6.6	Праздник Весны и Труда	01 мая
6.7	День Победы	09 мая
6.8	День защиты детей	01 июня
6.9	День России	12 июня
6.10	День Памяти и скорби	Июнь
6.11	День любви, семьи и верности	Июль

Раздел 3. Список литературы

Литература для педагогов:

1. Морозов В.А. Кибербезопасность для школьников: учебно-методическое пособие / В.А. Морозов. — Москва: Просвещение, 2019. — 96 с.;
2. Иванова Е.П. Безопасность ребёнка в интернете: практическое пособие для родителей и педагогов / Е.П. Иванова. — Санкт-Петербург: БХВ-Петербург, 2020. — 128 с.;
3. Смирнов А.С. Основы информационной культуры и цифровой безопасности: учебное пособие для учащихся / А.С. Смирнов. — Москва: Академия, 2018. — 112 с.;
4. Терехова Н.В. Правила безопасного поведения в сети для детей и подростков: практическое руководство / Н.В. Терехова. — Москва: Эксмо, 2021. — 80 с.;
5. Центр безопасного интернета. Методические рекомендации по формированию навыков кибербезопасности у детей и подростков [Электронный ресурс] / Минкомсвязь России, Центр безопасного интернета. — Режим доступа: https://www.safeinternet.ru/ (дата обращения: 14.01.2026).
6. Роскомнадзор. Правила безопасного поведения в сети для детей и подростков [Электронный ресурс]. — Режим доступа: https://rkn.gov.ru/ (дата обращения: 14.01.2026).
7. Кузнецова Л.М., Петухова И.В. Фишинг и интернет-мошенничество: как распознать и избежать / Л.М. Кузнецова, И.В. Петухова. — Москва: Вильямс, 2017. — 64 с.;
8. НИКСОН Д. Безопасность в интернете для детей: иллюстрированное пособие / Д. Никсон; пер. с англ. — Москва: Манн, Иванов и Фербер, 2016. — 96 с.;
9. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Методические материалы по информационной безопасности для образовательных организаций [Электронный ресурс]. — Режим доступа: https://rkn.gov.ru/education/ (дата обращения: 14.01.2026).
10. Химичев С.В. Цифровая гигиена и защита персональных данных: рабочая тетрадь для школьников / С.В. Химичев. — Москва: Учитель, 2022. — 48 с.;
11. Иванов П.А. Проверка фактов и распознавание фейков в школьной практике: методическое пособие / П.А. Иванов. — Санкт-Петербург: Речь, 2020. — 72 с.;
12. Баранов И.И. Кибербезопасность в школе: сборник кейсов и упражнений / И.И. Баранов. — Москва: Детская книга, 2021. — 88 с.;
13. Федеральный закон Российской Федерации от 27.07.2006 N 152-ФЗ «О персональных данных» : текст законопроекта [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 14.01.2026).

Приложение 1

Календарный учебный график

№	Дата	Месяц	Тема	Кол-во часов	Формы контроля
1.		январь	Введение в кибербезопасность. ТБ	1	Опрос наблюдение
2.		январь	Личные данные: что можно и что нельзя публиковать.	1	Опрос по теме Выполнение практического задания
3.		февраль	Пароли: как придумывать и хранить.	1	Опрос по теме Выполнение практического задания
4.		февраль	Фишинг: письма, ссылки и поддельные сайты	1	Опрос по теме Выполнение практического задания
5.		февраль	Социальные сети и общение онлайн	1	Опрос по теме Выполнение практического задания
6.		февраль	Безопасность фотографий и геометки	1	Опрос по теме Выполнение практического задания
7.		март	Безопасность на мобильных устройствах	1	Опрос по теме Выполнение практического задания
8.		март	Вредоносное ПО: вирусы, трояны, шпионское ПО	1	Опрос по теме Выполнение практического задания
9.		март	Электронная почта: правила использования и безопасность	1	Опрос по теме Выполнение практического задания
10.		март	Проверка информации и медиаграмотность	1	Опрос по теме Выполнение практического задания
11.		апрель	Игры и внутриигровые покупки: безопасность и время	1	Опрос по теме Выполнение практического задания
12.		апрель	Что делать при кибербуллинге и угрозах	1	Опрос по теме Выполнение практического задания
13.		апрель	Основы авторских прав и безопасное использование контента	1	Опрос по теме Выполнение практического задания

14.		апрель	Создание цифрового следа и репутация	1	Опрос по теме Выполнение практического задания
15.		май	Основы защиты устройств: антивирусы, пароли на устройствах, шифрование	1	Опрос по теме Выполнение практического задания
16.		май	Заключительное занятие	1	Квест-игра
ИТОГО:				16	

Приложение 2

Анкета о привычках в сети Интернет.

Твои ответы помогут сделать интернет безопаснее и интереснее для всех ребят.

1. **Сколько времени** ты проводишь в интернете каждый день?
   - Менее 30 минут
   - 30-60 минут
   - 1-2 часа
   - Более 2 часов
2. **Какие сайты** ты чаще всего посещаешь? (можно выбрать несколько вариантов)
   - Социальные сети
   - Образовательные платформы
   - Игры
   - Видеохостинги
   - Другое (укажите) _____
3. **С кем** ты обычно общаешься в интернете?
   - С друзьями из школы
   - С новыми знакомыми
   - С родственниками
   - Один
4. **Как часто** ты рассказываешь родителям о том, что делаешь в интернете?
   - Каждый день
   - Раз в неделю
   - Редко
   - Никогда
5. **Знаешь ли ты** правила безопасного поведения в интернете? (да/нет) Если да, то какие правила ты соблюдаешь?

_____

6. **Сталкивался ли** ты с неприятными ситуациями в сети? (например, кибербуллинг, мошенничество)
   - Да
   - Нет
   - Затрудняюсь ответить
7. **Что бы** ты хотел изменить в использовании интернета?

_____

8. **Какие приложения** тебе нравятся больше всего?

_____

9. **Помогают ли** родители тебе разобраться в сложных ситуациях в интернете?

- Всегда помогают
- Иногда помогают
- Никогда не помогают

10. **Хотел бы** ты научиться чему-то новому с помощью интернета? Если да, то чему?

_____

Спасибо за участие в опросе! Твои ответы очень важны для нас.

Тест для обсуждения: «Как Даша подарком воспользовалась»

Цель: обучение детей правильно оценивать свои и чужие поступки.

Сегодня я расскажу вам реальную историю про маленькую девочку Дашу. Жила девочка Даша, и она очень хотела на Новый год компьютер, но пользоваться компьютером Даша не умела. Наконец Дарья дождалась подарка. Компьютер был черного цвета и очень большой. Как-то раз Даша решила зайти с компьютера на страницу в контакте. Зашла, почитала новости, посмотрела фотографии подружек. Подружка Нина была в сети, и Даше захотелось с ней пообщаться. Девочки начали свой разговор смайликами. Даша удивилась, как Нина отправляет такие красивые и необычные смайлики. Даша спросила у Нины: «Как ты, отправляешь такие смайлики?». Нина быстро ответила: «Родители купили». Даше не понравилось, что Нине купили такие милые смайлики, а ей нет. Даша зашла на страницу, где продавались смайлики, и нажала на кнопку «Купить». Чуть позже высветилась таблица, на ней было написано: «Укажите номер своего телефона». И много другой информации» запрашивали, но Даша ничего читать не стала, а просто написала номер своего телефона и начала ждать, когда у неё будут такие смайлики. Даше на телефон пришло смс сообщение: «Вы купили смайлики. Спасибо за покупку!». Через некоторое время Даше пишет мама смс сообщение: «Ты уже дома?» Даша только начинает отправлять сообщение, а ей высвечивается сообщение: «Недостаточно средств на телефоне». Вечером приходит мама и спрашивает: «Почему ты не ответила на смс сообщение?». Даша отвечает: «Потому что у меня нет денег на телефоне». Мама удивилась: «Так я тебе вчера только деньги на телефон положила!». Даша опустила глаза и рассказала, что случилось. Больше Даша никогда без разрешения взрослых ничего не покупала!

Вопросы для обсуждения:

- Сравните поступок Даши после покупки компьютера?
- Как отнеслась мама к поведению дочери?
- Нина могла остановить каким-образом Дашу?

Дети обсуждают варианты поведения в этой ситуации.

Подведение итогов. Педагог еще раз акцентирует внимание детей на ситуации, рассмотренной на классном часе, делает выводы:

1. Слушаться взрослых:

2. Совершать покупки могут только взрослые члены семьи.

3. Игры на компьютере, планшете, в телефоне должны быть дозированными по времени.

Приложение 3

Мини-тест «Надежность пароля».

1. **Что такое пароль?**
   - Слово, которое нужно вводить для подтверждения личности или полномочий.
   - Имя пользователя в социальной сети.
   - Номер телефона.

2. **Какой минимальной длины должен быть хороший пароль?**
   - 6 символов.
   - 8 символов.
   - 10 символов.

3. **Сколько наборов символов должен содержать сложный пароль?**
   - Один набор.
   - Два набора.
   - Три набора.

4. **Какие наборы символов должен содержать надежный пароль?**
   - Большие и маленькие буквы.
   - Цифры.
   - Специальные символы.
   - Все вышеперечисленные.

5. **Как лучше хранить пароль?**
   - в памяти.
   - на листочке бумаги.
   - в менеджере паролей.

6. **Сколько символов должен содержать надежный пароль?**
   - не менее 4 символов.
   - не менее 8 символов.
   - не менее 12 символов.

7. **Можно ли использовать для пароля общедоступную информацию, такую как имя, фамилию, важные даты и т.д.?**
   - да, можно.
   - нельзя, это не безопасно.

8. Какой из следующих паролей является надёжным?

- 123456
- Qwerty123
- Rsdvbjkgd2#bn4f!

9. Можно ли использовать один и тот же пароль для разных сайтов?

- Да, можно.
- Нет, нельзя.

10. Какой пароль был назван худшим по данным на 2024 год, по версии исследователей NordPass?

- Password
- 123456
- Asdfghj

Итоги:

0 – 2 балла — Уровень «Начинающий» (Звание: «Новичок сети»).

Описание: имеются серьёзные пробелы в базовых знаниях кибербезопасности.

3–5 баллов — Уровень «Базовый» (Звание: «Защитник начинающий»).

Описание: есть базовые представления, но часто допускаются ошибки при применении знаний.

6–8 баллов — Уровень «Уверенный» (Звание: «Киберстраж»).

Описание: хорошие знания и уверенное применение основных правил безопасности; редкие ошибки в сложных ситуациях.

9–10 баллов — Уровень «Эксперт» (Звание: «Кибергерой»).

Описание: отличное владение материалом, умеет распознавать и предотвращать большинство угроз; готов помогать другим и участвовать в квестах.

Пример упражнения: «Расследование фишинговой атаки».

Задача 1: Детектив получил подозрительное письмо по электронной почте с просьбой срочно подтвердить данные своей банковской карты. Как детектив должен поступить? Перечисли признаки, которые указывают на то, что это фишинговое письмо. (Умение распознавать фишинг).

Задача 2: Детектив увидел в интернете новость о том, что инопланетяне приземлились в их городе. Как детектив должен проверить, является ли эта новость правдивой? Перечисли основные шаги. (Навыки проверки информации).

Игра «Факт или вымысел».

У осьминога три сердца. Факт: главное сердце перекачивает кровь по всему телу, в то время как два других — по каждой из жабр.

У каждого человека есть уникальный отпечаток языка. Факт: даже у однояйцевых близнецов разные отпечатки языка.

Вы не можете напевать, зажимая нос. Факт: для напевания требуется поток воздуха через нос.

Банан — это ягода, а клубника — нет. Факт: банан квалифицируется как ягода, а клубника — нет, потому что его семена находятся снаружи.

Венера — единственная планета, которая вращается по часовой стрелке. Факт.

Великая Китайская стена видна из космоса. Вымысел: это не видно невооружённым глазом.

У ягуаров самый сильный прикус в животном мире, но самые маленькие зубы. Вымысел: у морского крокодила самый крепкий прикус и самые маленькие зубы.

У людей раньше были жабры на самых ранних стадиях развития. Вымысел: у них развиваются глоточные мешочки или жаберные щели.

Поп-рок с содовой заставят желудок взорваться. Вымысел: это может вызвать газы и отрыжку, но не взрыв желудка.

Приложение 4

Квест-игра «БезОпасный Интернет»

Цель: помочь овладеть эффективными способами грамотного использования интернета в рамках познавательной и досуговой деятельности школьников начального и среднего звена.

Задачи:

- систематизировать знания детей в области интернет-безопасности,
- формировать у детей навыки безопасного использования интернета.

Участники: команда учащиеся с 1 по 6 класс, состоящая из 10 человек.

Форма организации работы: групповая.

Оборудование и материалы:

Дидактические материалы (маршрутные листы, раздаточный материал для станции), лист ватмана, кисти, краски, фломастеры, ножницы, клей, вырезки из газет и журналов с изображениями по теме квест-игры.

Ход:

Ввод в игру:

Встреча и приветствие команд. Знакомство участников с темой правилами игры.

Правила игры:

1. Каждая команда проходит **5 станции.** На каждой станции команда выполняет предложенные теоретические и практические задания, о чем ставится отметка в маршрутном листе.
2. На каждом этапе находятся модераторы, которые следят за правильностью выполнения заданий и ставят отметку в маршрутном листе о его выполнении.
3. Прохождение станции выполняется строго по указанным станциям в маршрутных листах.
4. После прохождения всех этапов маршрутные листы сдаются членам жюри для оценки.
5. В конце игры побеждает команда, набравшая наибольшее количество баллов.

На данном этапе командам выдаются маршрутные листы *(Приложение1)*

Первая станция «Осторожно ВИРУСЫ!»

Необходимо уничтожить злой вирус *(Приложение 2)* стрелами Касперского, попав в него с расстояния. Число попаданий = числу баллов.

Каспе́рский - российский программист, один из ведущих мировых специалистов в сфере информационной безопасности. Человек, разработавший антивирусную программу для компьютеров и ноутбуков.

Стрелы необходимо заработать, для этого предложенную измененную пословицу вы должны интерпретировать в русскую народную пословицу. За каждый правильный ответ вы получаете стрелу Касперского.

Перед вам на столе лежат пословицы, вытягивайте любую (всего можно вытянуть 5 штук).
Пословицы для перевода в русскую народную *(Приложение 3)*

Вторая станция: «Запутанные термины»
- Ребята, перед вами слова и их определения, к сожалению они перепутались. Ваша задача, соединить термин с его определением. *(Приложение 4)*

Третья станция: «Филворд»
- Перед вами поле с засекреченными словами, ваша задача найти как можно больше слов связанных с интернетом, за каждое найденное слово вы зарабатывайте - 1 балл. *(Приложение 5)*

Четвертая станция: «Компьютерный крокодил»
- Одному человеку ответственный по станции загадывает слово, одному участнику команды, его задача с помощью мимики и жестов объяснить слово. Команде нужно отгадать как можно больше слов (от простых к сложным) по теме квеста *(Приложение 6)*. Одно отгаданное слово -1 балл.

Пятая станция: «Ребусы»
- Нужно отгадать ребусы по теме квеста *(Приложение 7)*. Один решенный ребус -1 балл.

Шестой этап: «Прояви фантазию»
Все команды собираются в одном месте и получают творческое задание: на листе ватмана придумать и изобразить знак безопасного интернета. В это время жюри подводит итоги.

Подведение итогов:
Определяются победители игры по наибольшему количеству баллов.
- Вот и подошла к завершению наша квест-игра “БезОпасный Интернет”. Благодарим вас за участие и дарим вам памятки «Безопасность в Интернете» *(Приложение 8)*.

Готовые плакаты размещаются на стенде школы для общей информированности учащихся.

Приложение 1

Маршрутный лист квест-игры «БезОпасный Интернет»

Станция	Название станции	Пункт следования	баллы
1	«Осторожно ВИРУСЫ!»	1	
2	«Запутанные термины»	2	
3	«Филворд»	3	
4	«Компьютерный крокодил»	4	
5	«Ребусы»	5	

Маршрутный лист квест-игры «БезОпасный Интернет»

Станция	Название станции	Пункт следования	баллы
1	«Осторожно ВИРУСЫ!»	5	
2	«Запутанные термины»	1	
3	«Филворд»	2	
4	«Компьютерный крокодил»	3	
5	«Ребусы»	4	

Маршрутный лист квест-игры «БезОпасный Интернет»

Станция	Название станции	Пункт следования	баллы
1	«Осторожно ВИРУСЫ!»	4	
2	«Запутанные термины»	5	

3	«Филворд»	1	
4	«Компьютерный крокодил»	2	
5	«Ребусы»	3	

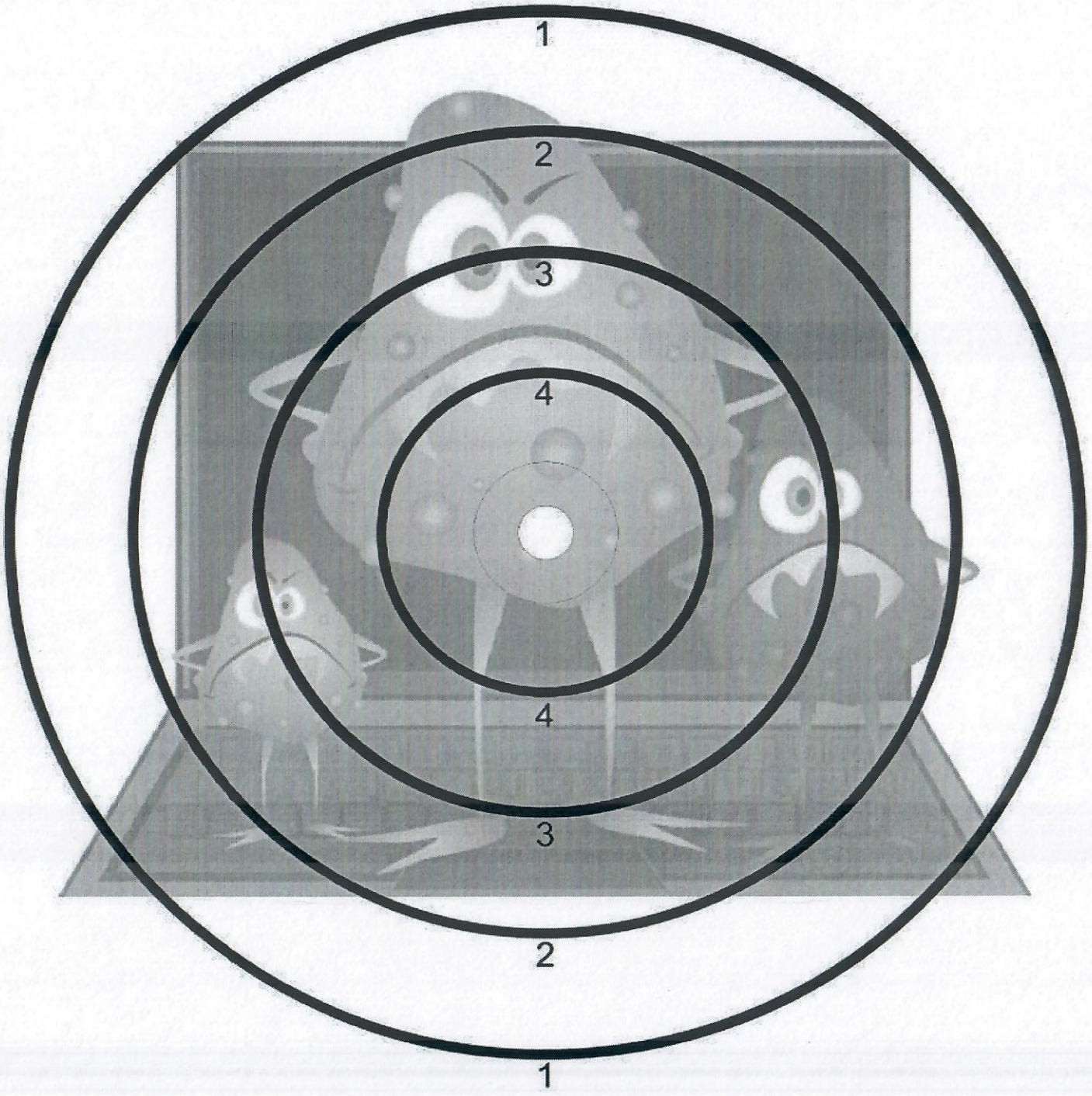
Маршрутный лист квест-игры «БезОпасный Интернет»

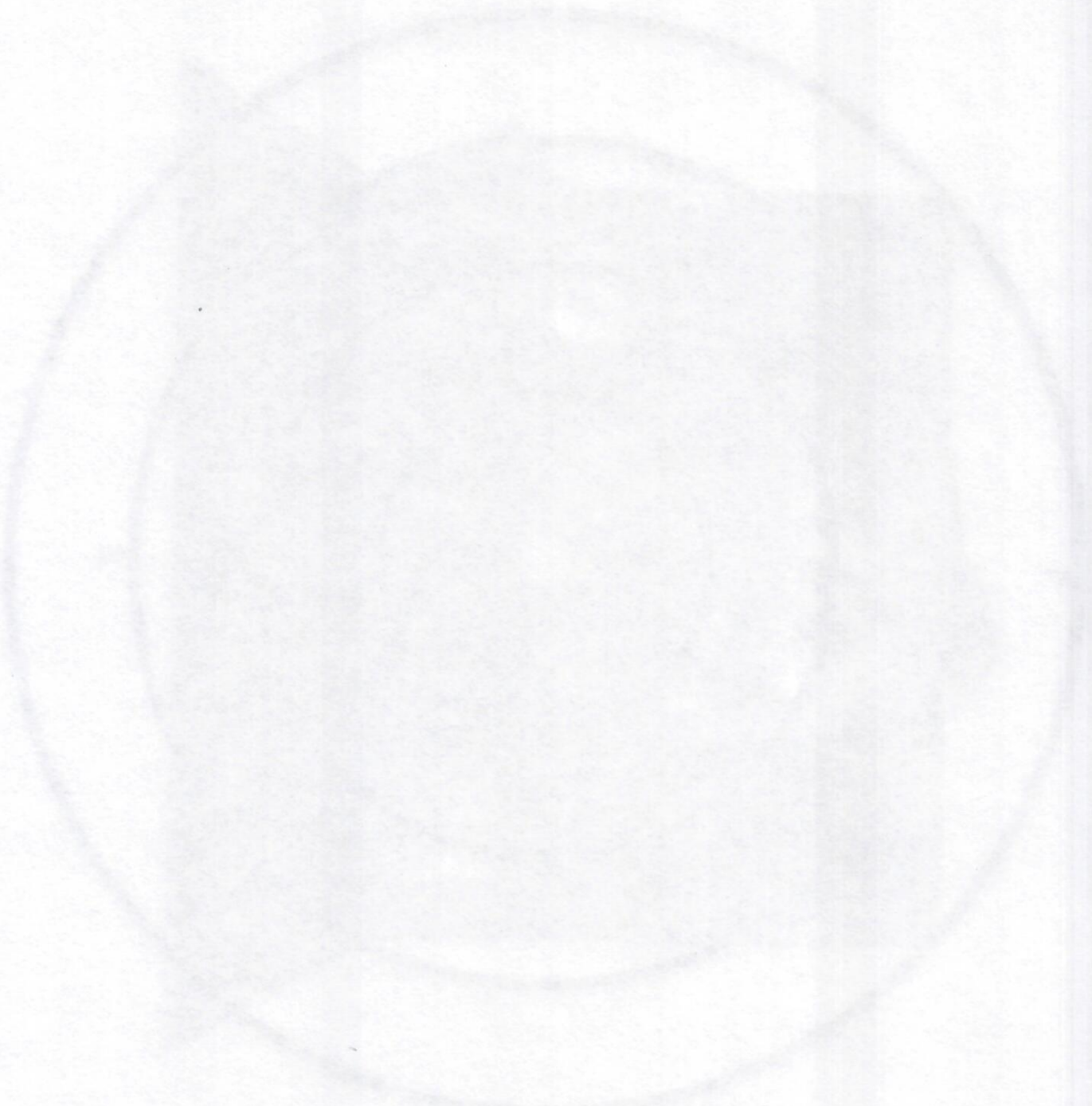
Станция	Название станции	Пункт следования	баллы
1	«Осторожно ВИРУСЫ!»	3	
2	«Запутанные термины»	4	
3	«Филворд»	5	
4	«Компьютерный крокодил»	1	
5	«Ребусы»	2	

Маршрутный лист квест-игры «БезОпасный Интернет»

Станция	Название станции	Пункт следования	баллы
1	«Осторожно ВИРУСЫ!»	2	
2	«Запутанные термины»	3	
3	«Филворд»	4	
4	«Компьютерный крокодил»	5	
5	«Ребусы»	1	

Приложение 2





Приложение 3

Задания	**Ответы**
Скажи мне, какой у тебя компьютер, и я скажу, кто ты.	**Скажи мне, кто твой друг, и я скажу, кто ты.**
Компьютер памятью не испортишь.	**Кашу маслом не испортишь.**
Дареному компьютеру в системный блок не заглядывают.	**Дареному коню в зубы не смотрят.**
В Силиконовую долину со своим компьютером не ездят.	**В Тулу со своим самоваром не ездят.**
Утопающий за F1 хватается.	**Утопающий за соломинку хватается.**
Бит байт бережет.	**Копейка рубль бережет.**
Что из Корзины удалено, то пропало.	**Что с возу упало, то пропало.**
Вирусов бояться – в Интернет не ходить.	**Волков бояться – в лес не ходить.**
За одного хакера семь кандидатов наук дают.	**За одного битого семь небитых дают.**
Всяк Web-дизайнер свой сайт хвалит.	**Всяк кулик свое болото хвалит.**

Приложение 4

Интернет	Всемирная компьютерная сеть, соединяющая вместе тысячи сетей.
Гиперссылка	Графическое изображение или текст на сайте, в письме электронной почты или в каком-либо электронном документе, выделяется, синим цветом и подчеркиванием.
Поисковые системы	Это сервисы, предназначенные для поиска информации в мировой сети Интернет. В базе данных поисковых систем находится информация, практически по любой теме.
Электронная почта	Технология и предоставляемые ею услуги по пересылке и получению электронных сообщений
Браузер	Средство просмотра веб-страниц.

Сетевой этикет	Нравственные правила поведения в компьютерных сетях.
Компьютерный вирус	Разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению.
Антивирусная программа	Любая программа для обнаружения компьютерных вирусов, а также нежелательных программ и восстановления зараженных такими программами файлов.

Приложение 5

И	О	М	И	Я	Р	У	С	М
Н	Д	Т	Ц	В	И	С	П	А
Т	Е	Е	А	Б	З	А	Д	О
С	Р	Н	М	Р	А	К	Д	М
А	И	Н	Р	А	К	Л	А	Е
Й	Т	Ф	О	У	З	Е	Р	Н

Приложение 6

Телефон
Вирус
Паутина
Ноутбук
Блоггер

Пароль
Ник
Социальная сеть

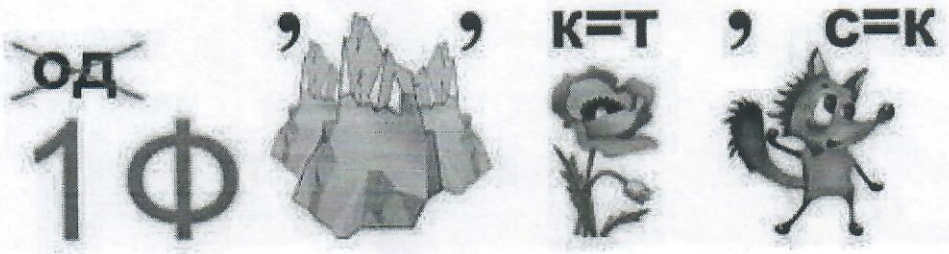
Приложение 7

Вирус

Интернет

Компьютер

Информатика



БЕЗОПАСНОСТЬ в Интернете

Не указывай свою личную информацию, настоящее имя, адрес, телефон и места, где ты часто бываешь.

Относись с осторожностью к публикации личных фото. Не выкладывай фото других людей без их согласия.

Не доверяй всей информации, размещенной в Интернете. Не доверяй незнакомым людям, они могут выдавать себя за других.

Не переходи по сомнительным ссылкам (например, обещающим выигрыш). Не посещай сомнительные сайты. Они могут нанести вред твоей психике.

Помни, что незаконное копирование авторских материалов преследуется по закону.

Не встречайся в реальной жизни с людьми, с которыми ты познакомился в Интернете. Сообщи родителям, если друзья из Интернета настаивают на личной встрече.

Помни, что в виртуальном мире действуют те же правила вежливости, что и в реальном.

Не отправляй смс, чтобы получить какую-либо услугу или выиграть приз.

Обращайся за советом к взрослым при малейшем сомнении или подозрении.