

МИНИСТЕРСТВО ОБРАЗОВАНИЯ НОВОСИБИРСКОЙ ОБЛАСТИ

муниципальное бюджетное общеобразовательное
учреждение – лицей г. Татарска
(МБОУ - ЛИЦЕЙ)

РАССМОТРЕНО

на педагогическом совете

МБОУ – ЛИЦЕЯ

протокол № 1 от 27.08.2026

УТВЕРЖДАЮ
Директор
МБОУ – ЛИЦЕЯ
_____ Т.А. Чернова
приказ № 62/1/ОД от 27.08.2026



**ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ
ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА
«Кибербезопасность и защита данных: шаг вперед»**

Направленность: техническая

Возраст обучающихся: 8-11 лет

**Автор: Семенова Наталья Николаевна,
педагог дополнительного образования**

Татарск– 2026

1.1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа «Кибербезопасность и защита данных в цифровой среде» разработана в соответствии с требованиями нормативных документов:

- Конституция Российской Федерации (от 12.12.1993 с изм. 01.07.2020);
- Указ Президента Российской Федерации от 21.07.2020 «О национальных целях развития РФ на период до 2030 года»;
- Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности РФ»;
- Указ Президента Российской Федерации от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей»;
- Федеральный Закон от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации» (далее – ФЗ-273);
- Федеральный закон РФ от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;
- Федеральный закон от 30.04.2021 г. № 127-ФЗ «О внесении изменений в Федеральный закон «О физической культуре и спорте в Российской Федерации» и в Федеральный закон «Об образовании в Российской Федерации» (далее - ФЗ-127);
- Федеральный закон «О российском движении детей и молодежи» от 14.07.2022 №261-ФЗ (далее- ФЗ-261);
- Стратегия развития воспитания в РФ на период до 2025 года (распоряжение Правительства РФ от 29 мая 2015 г. № 996-р);
- Стратегическое направление в области цифровой трансформации образования, относящейся к сфере деятельности Министерства просвещения Российской Федерации (утв. распоряжением Правительства РФ от 02.12.2021 № 3427);
- Концепция развития дополнительного образования детей до 2030 года (утв. распоряжением Правительства РФ от 31.03.2022 № 678) (далее - Концепция);
- Постановление Главного государственного санитарного врача РФ от 28.09.2020 N 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи»;
- Постановление Главного государственного санитарного врача РФ от 28.01.2021 № 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» (рзд. VI. Гигиенические нормативы по устройству, содержанию и режиму работы организаций воспитания и обучения, отдыха и оздоровления детей и молодежи»);
- Федеральные проекты «Цифровая образовательная среда», «Современная школа», «Патриотическое воспитание» (2020);
- Паспорт федерального проекта «Успех каждого ребенка» (утвержден на заседании проектного комитета по национальному проекту «Образование» 07 декабря 2018 г., протокол № 3);
- Приказ Министерства образования и науки Российской Федерации от 23.08.2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных

технологий при реализации образовательных программ»;

- Приказ Министерства просвещения Российской Федерации от 03.09.2019 № 467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей»;

- Приказ министерства образования и науки Российской Федерации и министерства просвещения Российской Федерации от 5.08.2020 г. № 882/391 «Об организации и осуществлении образовательной деятельности по сетевой форме реализации образовательных программ»;

- Приказ Министерства просвещения Российской Федерации от 13.03.2019 № 114 «Об утверждении показателей, характеризующих общие критерии оценки качества условий осуществления образовательной деятельности организациями, осуществляющими образовательную деятельность по основным общеобразовательным программам, образовательным программам среднего профессионального образования, основным программам профессионального обучения, дополнительным общеобразовательным программам»;

- Приказ Министерства труда и социальной защиты Российской Федерации от 22.09.2021 № 652н «Об утверждении профессионального стандарта «Педагог дополнительного образования детей и взрослых»;

- Приказ Министерства просвещения Российской Федерации от 27.07.2022 г. № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

- Концепция развития креативных индустрий в Новосибирской области (утв. постановлением Правительства НСО от 08.06.2021 № 212-П);

- Устав МБОУ — ЛИЦЕЯ, утверждённый администрацией Татарского района Новосибирской области № 306 от 16.12.2015 г.

Методические рекомендации:

- Методические рекомендации по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы) (разработанные Минобрнауки России совместно с ГАОУ ВО «Московский государственный педагогический университет», ФГАУ «Федеральный институт развития образования», АНО ДПО «Открытое образование», 2015 г.) (Письмо Министерства образования и науки РФ от 18.11.2015 № 09-3242);

- Методические рекомендации по созданию и функционированию центров цифрового образования «IT-куб» (утв. распоряжением Министерства просвещения Российской Федерации от 29.03.2023 № АБ – 1339/02);

- Методические рекомендации по реализации дополнительных общеобразовательных программ с применением электронного обучения и дистанционных образовательных технологий (письмо Министерства просвещения РФ от 31.01.2022 № ДГ-245/06);

- Методические рекомендации «Об использовании государственных символов Российской Федерации при обучении и воспитании детей и молодежи в образовательных организациях, а также в организациях отдыха детей и их оздоровления» (письмо Министерства просвещения России от 15.04.2022 № СК-295/06);

- Примерная рабочая программа воспитания для общеобразовательных организаций, разработанная Институтом изучения семьи, детства и воспитания РАО по заданию Министерства

просвещения РФ, одобрена на заседании Федерального учебно-методического объединения по общему образованию 23 июня 2022 года (<https://xn--80adrabb4aegksdjbafk0u.xn--p1ai/programmy-vospitaniya/>);

- Примерная программа воспитания для дошкольных образовательных организаций и методические рекомендации к ней разработаны Институтом изучения детства, семьи и воспитания РАО по заданию Министерства просвещения РФ. 1 июля 2021 года программа была утверждена на заседании Федерального учебно-методического объединения по общему образованию (<https://xn--80adrabb4aegksdjbafk0u.xn--p1ai/programmy-vospitaniya/>);

- Приоритетные направления по обновлению содержания и технологий ДОД по всем направленностям (Рекомендованы экспертным советом министерства просвещения РФ по вопросам ДО детей и взрослых, воспитания и детского отдыха);

- Основы патриотического воспитания граждан Российской Федерации. Методические рекомендации (утв. Экспертным советом по патриотическому воспитанию при ФГБУ «Роспатриотцентр» 10.10.2022) (<https://www.rospatriotcentr.ru/>);

- Цифровой методический конструктор организатора воспитательной работы в школе (https://static.edsoo.ru/methodic_book/index.html).

Содержание программы «Кибербезопасность и защита данных в цифровой среде» поможет освоить азы интернет - безопасности и этикета в сети, ребята научатся быстро и эффективно искать информацию в глобальной сети, анализировать группы в социальных сетях, освоят основы защиты персональных данных и будут понимать угрозы информационной безопасности.

Уровень общеобразовательной программы: начальный

Направленность программы: техническая

Актуальность программы

Современные дети 8–11 лет активно используют цифровые устройства, Интернет, онлайн-игры, образовательные платформы, мессенджеры и различные цифровые сервисы. По мере расширения самостоятельности ребёнка увеличивается и количество ситуаций, в которых ему необходимо самостоятельно принимать решения в цифровой среде: оценивать достоверность информации, распознавать подозрительные сообщения и ссылки, защищать персональные данные, соблюдать правила общения и учитывать последствия своих действий в сети.

Актуальность программы обусловлена необходимостью формирования у обучающихся устойчивых навыков безопасного, осознанного и ответственного поведения в цифровой среде. Программа позволяет не только познакомить детей с основными правилами кибербезопасности, но и сформировать практические умения, которые необходимы им в повседневной цифровой деятельности.

Особое значение имеет развитие навыков противодействия интернет-мошенничеству, фишингу, кибербуллингу, распространению недостоверной информации и другим цифровым угрозам. Полученные знания и навыки помогут обучающимся более уверенно и безопасно использовать современные цифровые технологии для обучения, общения и творчества.

Новизна программы

Новизна программы заключается в сочетании основ цифровой грамотности и кибербезопасности с практической деятельностью обучающихся. Изучение материала строится не только на получении теоретических знаний, но и на разборе жизненных ситуаций, выполнении практических заданий, моделировании различных цифровых угроз и поиске способов безопасного поведения.

Возраст обучающихся 8–11 лет позволяет постепенно переходить от простого ознакомления с правилами безопасности к осознанному анализу цифровых ситуаций и самостоятельному принятию решений. В программе большое внимание уделяется развитию критического мышления, информационной грамотности, ответственности за собственные действия и пониманию понятия «цифровой след».

Игровые и интерактивные формы работы позволяют сделать изучение вопросов кибербезопасности доступным и интересным для детей, одновременно формируя навыки, необходимые для безопасного использования цифровых технологий.

Отличительные особенности программы

Программа разработана с учетом возрастных и психологических особенностей детей 8–11 лет и ориентирована на постепенное повышение уровня их самостоятельности в цифровой среде.

Содержание программы связано с реальными цифровыми ситуациями, с которыми обучающиеся могут столкнуться при использовании Интернета, онлайн-игр, мессенджеров, образовательных платформ и других сервисов.

Значительное место занимают практические задания, позволяющие закреплять правила безопасного поведения и отрабатывать алгоритмы действий в различных ситуациях.

Используются интерактивные методы обучения: игровые задания, викторины, кейсы, дискуссии, моделирование проблемных ситуаций, командная и групповая работа.

Особое внимание уделяется развитию критического мышления и информационной грамотности: обучающиеся учатся отличать достоверную информацию от недостоверной, выявлять признаки обмана, манипуляции и фишинга.

Рассматриваются вопросы защиты персональных данных, создания надежных паролей, безопасного общения в сети, цифрового следа и ответственного поведения при публикации материалов в Интернете.

Программа способствует формированию культуры общения в цифровой среде, развитию эмпатии и навыков конструктивного поведения при возникновении конфликтных ситуаций и кибербуллинга.

Использование офисного пакета Р7 позволяет обучающимся осваивать отечественные цифровые инструменты и одновременно развивать практические навыки работы с текстовыми документами, электронными таблицами и презентациями.

Адресат программы

Программа рассчитана на детей 8 – 11 лет.

Обучающиеся данного возраста активно используют цифровые устройства и Интернет не только под контролем взрослых, но и самостоятельно. Они интересуются онлайн-играми, видеоконтентом, образовательными ресурсами, мессенджерами и различными цифровыми сервисами, активно взаимодействуют со сверстниками в виртуальном пространстве.

В этом возрасте у детей формируется способность к более осознанной оценке информации и последствий собственных действий, однако они по-прежнему нуждаются в систематическом формировании навыков безопасного поведения в цифровой среде. Недостаток

опыта может привести к необдуманному раскрытию персональной информации, переходу по подозрительным ссылкам, общению с незнакомыми людьми, вовлечению в конфликтные ситуации или распространению недостоверной информации.

Содержание программы учитывает возрастные особенности обучающихся и направлено на развитие самостоятельности, ответственности и критического отношения к происходящему в цифровой среде. Практико-ориентированный характер занятий позволяет обучающимся не только узнать о возможных цифровых угрозах, но и научиться правильно действовать при их возникновении

Объём и срок освоения программы

Объём программы - 72 часа в год.

Программа рассчитана на 1 год обучения.

Форма обучения: очная.

Режим занятий, периодичность и продолжительность занятий

Занятия проводятся два раза в неделю продолжительностью 2 академических часа (1 академический час равен 45 минутам). Перерыв между учебными занятиями 10-15 минут.

Количество обучающихся в одной группе 10-12 человек.

1.2 ЦЕЛИ И ЗАДАЧИ ПРОГРАММЫ

Цель программы: формирование у обучающихся 8–11 лет практических навыков безопасного, осознанного и ответственного использования цифровых технологий, Интернета и цифровых сервисов.

Задачи программы:

Образовательные:

1. сформировать представление о цифровой среде, основных цифровых угрозах и принципах кибербезопасности;
2. научить распознавать признаки вредоносных файлов, подозрительных сообщений, фишинговых страниц и интернет-мошенничества;
3. сформировать навыки защиты персональных данных, аккаунтов и цифровых устройств;
4. познакомить с правилами безопасного общения в социальных сетях, мессенджерах и онлайн-играх;
5. сформировать представление о цифровом следе, приватности и последствиях публикации информации в сети;
6. научить проверять информацию из интернет-источников и выявлять признаки фейков, манипуляций и недостоверного контента;
7. познакомить с базовыми возможностями офисного пакета Р7 и правилами безопасной работы с документами, таблицами и презентациями.

Развивающие:

1. развивать критическое и алгоритмическое мышление;
2. развивать умение анализировать цифровые ситуации, сравнивать варианты действий и выбирать безопасное решение;

3. развивать навыки поиска, проверки, систематизации и представления информации;
 4. развивать коммуникативные навыки, умение аргументировать позицию и работать в команде;

5. развивать навыки самоорганизации и ответственного планирования собственной деятельности в цифровой среде.

Воспитательные:

6. воспитывать ответственное отношение к собственным действиям и информации в цифровой среде;

7. формировать уважительное и этичное поведение при онлайн-общении;

8. воспитывать уважение к персональным данным и цифровым правам других людей;

9. формировать неприятие травли, унижения, мошенничества и иных форм небезопасного поведения в сети;

10. формировать культуру безопасного и осознанного использования цифровых технологий.

1.3 СОДЕРЖАНИЕ ПРОГРАММЫ

Учебный план

№ п/п	Название раздела	Количество часов		
		всего	из них	
			теория	практика
1.	Цифровая среда и основы кибербезопасности	4	1	3
2.	Вредоносное ПО, вирусы и безопасная работа с файлами	6	2	4
3.	Безопасный Интернет: сайты, ссылки и фишинг	8	2	6
4.	Персональные данные, аккаунты и цифровой след	8	2	6
5.	Кибербуллинг и психологическая безопасность	8	2	6
6.	Безопасное онлайн-общение и цифровой этикет	8	2	6
7.	Безопасность в онлайн-играх и цифровых сервисах	6	1	5
8.	Критическое мышление и проверка информации	8	2	6
9.	Офисный пакет Р7: документы, таблицы и презентации	16	4	12
	ИТОГО:	72	18	54

Содержание программы

Раздел 1. Цифровая среда и основы кибербезопасности (4 часа)

Задачи:

1. понимать, что такое цифровая среда и кибербезопасность;
 2. знать основные виды цифровых устройств и сервисов;
 3. понимать, почему безопасность зависит не только от устройства, но и от действий пользователя.

Теория (1 час):

Устройство современной цифровой среды. Интернет, сайты, приложения, аккаунты и цифровые сервисы. Основные цифровые угрозы. Правила безопасной работы за компьютером и с мобильными устройствами.

Практика (3 часа):

Кейс «Безопасный цифровой день»; классификация цифровых устройств и сервисов; разбор ситуаций «Что может быть опасным?»; составление алгоритма действий при возникновении подозрительной ситуации.

Раздел 2. Вредоносное ПО, вирусы и безопасная работа с файлами (6 часов)

Задачи:

1. знать основные виды вредоносного программного обеспечения;
2. распознавать типичные признаки подозрительных файлов и сообщений;
3. понимать назначение антивирусных средств и обновлений;
4. соблюдать правила безопасной работы с файлами и внешними носителями.

Теория (2 часа):

Вредоносное программное обеспечение: вирусы, трояны, шпионские программы и другие виды угроз. Пути распространения. Антивирусная защита. Обновления. Безопасная загрузка файлов.

Практика (4 часа):

Анализ безопасных учебных примеров вредоносных сообщений; игра «Кибердетектив»; проверка признаков подозрительного файла; составление алгоритма «Остановись — проверь — сообщи»; практическое моделирование действий при обнаружении угрозы.

Раздел 3. Безопасный Интернет: сайты, ссылки и фишинг (8 часов)

Задачи:

1. различать образовательные, информационные, развлекательные и другие ресурсы;
2. оценивать надёжность сайта и ссылки по совокупности признаков;
3. распознавать основные признаки фишинга;
4. безопасно пользоваться поиском и не переходить по подозрительным ссылкам.

Теория (2 часа):

Типы сайтов. Адрес сайта и доменное имя. Защищённое соединение как один из признаков, но не единственный критерий доверия. Фишинговые сайты и сообщения. Подозрительные ссылки, формы входа и предложения.

Практика (6 часов):

Квест «Киберстража»; сравнение учебных примеров сайтов; анализ ссылок; поиск признаков фишинга; создание чек-листа проверки сайта; кейсы «Мне пришла подозрительная ссылка»; безопасный поиск информации.

Раздел 4. Персональные данные, аккаунты и цифровой след (8 часов)

Задачи:

1. различать персональные и общедоступные сведения;
2. создавать и оценивать надёжность паролей;
3. понимать назначение двухфакторной аутентификации;
4. понимать, что публикации формируют цифровой след;
5. выбирать безопасные настройки приватности.

Теория (2 часа):

Персональные данные. Пароли и парольные фразы. Повторное использование паролей и связанные риски. Двухфакторная аутентификация. Приватность. Цифровой след. Безопасная регистрация в цифровых сервисах.

Практика (6 часов):

Игра «Что можно публиковать?»; конструктор надёжной парольной фразы без использования реальных паролей; анализ учебных профилей; настройка приватности на учебном примере; кейс «Фото уже опубликовано»; создание памятки «Мой цифровой след».

Раздел 5. Кибербуллинг и психологическая безопасность (8 часов)

Задачи:

1. различать конфликт, шутку, травлю и кибербуллинг;
2. распознавать признаки психологически небезопасного общения;
3. знать безопасный алгоритм действий при столкновении с травлей;
4. понимать роль свидетеля и способы оказания поддержки без эскалации конфликта.

Теория (2 часа):

Понятие кибербуллинга. Формы проявления: оскорбления, угрозы, распространение унижительных материалов, исключение из цифрового общения. Эмоциональные последствия. Безопасное обращение за помощью. Сохранение доказательств и блокировка нарушителя.

Практика (6 часов):

Ролевые кейсы; анализ переписок на учебных примерах; составление алгоритма помощи; тренинг ответов без конфронтации; работа в группах «Что делать свидетелю?»; создание цифрового плаката о безопасном общении.

Раздел 6. Безопасное онлайн-общение и цифровой этикет (8 часов)

Задачи:

1. соблюдать правила цифрового этикета;
2. понимать риски общения с незнакомыми людьми;
3. оценивать последствия публикации сообщений, фотографий и комментариев;
4. уметь использовать функции блокировки и жалобы в учебных моделях сервисов.

Теория (2 часа):

Цифровой этикет. Тон и контекст онлайн-сообщений. Общение с незнакомцами. Приватность. Публикация фотографий и сообщений. Блокировка, жалоба и обращение к взрослому.

Практика (6 часов):

Разбор диалогов; игра «Отправлять или не отправлять?»; моделирование общения; анализ комментариев; составление правил группы; практические задания по выбору безопасного действия в проблемной ситуации.

Раздел 7. Безопасность в онлайн-играх и цифровых сервисах (6 часов)

Задачи:

1. знать основные риски в онлайн-играх;
2. распознавать попытки получить пароль, код или доступ к аккаунту;
3. понимать риски виртуальных покупок и сомнительных предложений;
4. соблюдать правила безопасного общения с игроками.

Теория (1 час):

Аккаунт игрока. Игровые чаты. Незнакомые пользователи. Мошенничество, фальшивые подарки и предложения. Защита игровых аккаунтов. Покупки и внутриигровые предметы. Баланс онлайн- и офлайн-активности.

Практика (6 часов):

Разбор игровых кейсов; игра «Это подарок или ловушка?»; моделирование общения с незнакомым игроком; анализ сообщений о выигрыше; составление правил безопасного игрового аккаунта; командная викторина.

Раздел 8. Критическое мышление и проверка информации (8 часов)

Задачи:

1. различать факт, мнение, рекламу и предположение;
2. выявлять признаки недостоверной информации;
3. проверять сведения по нескольким источникам;
4. распознавать эмоциональные и рекламные манипуляции.

Теория (2 часа):

Фейковые новости и недостоверные сообщения. Источник информации. Дата и автор. Сравнение нескольких источников. Заголовки и эмоциональные формулировки. Реклама, кликбейт и манипуляции.

Практика (6 часов):

Игра «Факт или вымысел?»; проверка учебных новостей; сравнение источников; анализ рекламных сообщений; поиск признаков кликбейта; создание алгоритма «Проверь информацию перед тем, как поверить и поделиться».

Раздел 9. Офисный пакет Р7: документы, таблицы и презентации (16 часов)

Задачи:

- знать назначение основных программ офисного пакета Р7;
- создавать и форматировать текстовые документы;
- создавать простые таблицы и презентации;
- соблюдать правила безопасного хранения и передачи файлов;
- представлять результаты собственной работы.

Теория (4 часа):

Состав офисного пакета Р7. Текстовый редактор, электронные таблицы, редактор презентаций. Форматирование. Работа с изображениями и таблицами. Безопасное имя файла и папки. Парольная защита там, где она предусмотрена. Безопасная передача документов и совместная работа.

Практика (12 часов):

Создание памятки в текстовом редакторе; оформление таблицы «Цифровые угрозы и способы защиты»; создание презентации «Безопасный Интернет»; работа с изображениями и источниками; подготовка итогового мини-проекта; защита проекта.

1.4 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ

Результативность программы определяется на основе компетентностного подхода с учётом возрастных возможностей обучающихся 8–11 лет.

Предметные результаты. Обучающиеся будут знать:

- основные понятия цифровой грамотности и кибербезопасности;
- основные виды цифровых угроз и способы защиты от них;
- правила работы с персональными данными, паролями и аккаунтами;
- признаки фишинга, мошеннических сообщений и подозрительных ссылок;
- правила безопасного поведения в социальных сетях, мессенджерах и онлайн-играх;
- понятие цифрового следа и основные правила цифровой приватности;
- признаки кибербуллинга и безопасный алгоритм действий при его возникновении;
- основные способы проверки достоверности информации;
- назначение и базовые возможности офисного пакета Р7.

Обучающиеся будут уметь:

- выбирать безопасную модель поведения в типичных цифровых ситуациях;
- распознавать признаки подозрительных сообщений, ссылок и файлов;
- создавать и оценивать надёжность парольных фраз;
- бережно относиться к персональным данным своим и других людей;
- использовать базовые настройки приватности и безопасного общения;
- действовать по алгоритму при столкновении с кибербуллингом или мошенничеством;
- проверять информацию по нескольким источникам;

- создавать простые документы, таблицы и презентации в Р7;
- работать над мини-проектом и представлять его результаты.

Метапредметные результаты:

Регулятивные:

- определять цель и последовательность выполнения учебной задачи;
- планировать работу и распределять время;
- оценивать результат и исправлять ошибки;
- соблюдать правила организации безопасного рабочего места.

Познавательные:

- искать, сравнивать, классифицировать и систематизировать информацию;
- анализировать цифровые ситуации и устанавливать причинно-следственные связи;
- выделять существенные признаки и делать выводы;
- использовать алгоритмы и схемы для решения учебных задач.

Коммуникативные:

- работать индивидуально и в группе;
- аргументированно выражать своё мнение;
- учитывать мнение других участников;
- задавать вопросы и конструктивно обсуждать проблемные ситуации;
- соблюдать нормы цифрового этикета.

Личностные результаты:

- осознание ответственности за собственные действия в цифровой среде;
- формирование культуры безопасного и осознанного использования цифровых технологий;
- уважительное отношение к другим пользователям;
- понимание ценности личной информации и необходимости её защиты;
- готовность обращаться за помощью при возникновении цифровых угроз;
- формирование критического отношения к информации и цифровому контенту.

2. КОМПЛЕКС ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИХ УСЛОВИЙ

2.1 КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Период обучения 36 недель, 2 часа в неделю. Всего занятий – 72

№ п/п занятия	Тема занятия	Форма занятия	Количество часов	Форма контроля
Раздел 1. Цифровая среда и основы кибербезопасности (4 часа)				
1	Цифровая среда: устройства, сервисы и аккаунты	Вводное занятие, анкетирование	2	КЗ
2	Основные цифровые угрозы и правила безопасного поведения. Игра «Киберстраж»	Лекция, практикум, игра	2	КЗ
Раздел 2. Вредоносное ПО, вирусы и безопасная работа с файлами (6 часов)				
1	Вредоносное программное обеспечение: виды и способы	Лекция, практикум, игра	2	КЗ

	распространения. Игра «Кибердетектив»			
2	Антивирусная защита и безопасная работа с файлами	Лекция, практикум	2	КЗ
3	Анализ подозрительных файлов и сообщений. Алгоритм «Остановись — проверь — сообщи»	Практикум, интерактивная игра	2	КЗ
Раздел 3. Безопасный Интернет: сайты, ссылки и фишинг (8 часов)				
1	Типы веб-сайтов и критерии оценки надёжности	Лекция, практикум	2	КЗ
2	Фишинг: признаки опасных сайтов, сообщений и ссылок	Лекция, практикум, квест	2	КЗ
3	Безопасный поиск информации и проверка ссылок	Практикум	2	КЗ
4	Анализ учебных примеров сайтов. Квест «Киберстража»	Практическая работа, игра	2	КЗ
Раздел 4. Персональные данные, аккаунты и цифровой след (8 часов)				
1	Персональные данные: что можно и нельзя публиковать	Лекция, кейсы, викторина	2	КЗ
2	Надёжные пароли и парольные фразы	Лекция, практикум	2	КЗ
3	Двухфакторная аутентификация и защита аккаунта. Игра «Защити аккаунт»	Практикум, игра	2	КЗ
4	Цифровой след и настройки приватности. Создание безопасного учебного профиля	Практикум, кейсы	2	КЗ
Раздел 5. Кибербуллинг и психологическая безопасность (8 часов)				
1	Кибербуллинг: формы, признаки и последствия	Лекция, практикум	2	КЗ
2	Как действовать при кибербуллинге. Ролевая игра	Практикум, ролевая игра	2	КЗ
3	Роль свидетеля: как безопасно оказать поддержку	Дискуссия, кейсы	2	КЗ
4	Создание памятки «Сеть без травли»	Проектная работа	2	ПР
Раздел 6. Безопасное онлайн-общение и цифровой этикет (8 часов)				
1	Цифровой этикет и уважительное общение	Лекция, практикум, игра	2	КЗ
2	Общение с незнакомыми людьми в сети	Лекция, практикум, ролевая игра	2	КЗ
3	Публикация фотографий, сообщений и комментариев: возможные последствия	Лекция, практическая работа	2	КЗ
4	Блокировка, жалоба и обращение за помощью. Анализ онлайн-диалогов	Практикум, кейсы	2	КЗ

Раздел 7. Безопасность в онлайн-играх и цифровых сервисах (6 часов)				
1	Правила безопасного поведения в онлайн-играх	Лекция, практикум	2	КЗ
2	Мошенничество в играх и защита игрового аккаунта	Лекция, практикум, кейсы	2	КЗ
3	Незнакомые игроки: анализ ситуаций и выбор безопасного поведения	Практикум, ролевая игра	2	КЗ
Раздел 8. Критическое мышление и проверка информации (8 часов)				
1	Факты, мнения и фейковые новости: как отличать достоверную информацию	Лекция, практикум	2	КЗ
2	Способы проверки информации и оценка источника	Лекция, практикум	2	КЗ
3	Кликбейт и манипуляции в рекламе	Практикум, анализ ситуаций	2	КЗ
4	Безопасная загрузка приложений. Алгоритм «Проверь перед установкой»	Лекция, практикум	2	КЗ
Раздел 9. Офисный пакет Р7: документы, таблицы и презентации (16 часов)				
1	Знакомство с офисным пакетом Р7. Обзор программ и правила безопасной работы	Лекция, практикум	4	КЗ
2	Текстовый редактор Р7: создание и форматирование документов. Работа над проектом «Правила кибербезопасности»	Лекция, практикум, проектная работа	4	КЗ
3	Электронные таблицы Р7: создание таблиц и представление данных. Работа над проектом	Лекция, практикум, проектная работа	2	КЗ
4	Редактор презентаций Р7: создание презентации «Безопасный Интернет». Работа над проектом	Лекция, практикум, проектная работа	4	КЗ
5	Защита итоговых проектов	Практикум, презентация	2	ПР

Календарный учебный график заполнен с помощью условных обозначений:

КЗ – комбинированные занятия, сочетающие элементы теории и практики;

ПР – проектная работа (работа над кейсами).

2.2 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Материально-техническое обеспечение программы:

- Компьютерное оборудование:

- Стационарные персональные компьютеры (системный блок, монитор, клавиатура USB, мышь USB) с доступом в интернет - 12 шт.(ноутбуки)
- Браузер «Google Chrome», «Mozilla Firefox» или «Яндекс Браузер».
- Пакет офисных программ «P7»
- Принтер цветной.
- интерактивная доска, проектор.

Кадровое обеспечение

1. Требования к кадровому обеспечению деятельности Центра «IT-куб» определяются образовательной организацией самостоятельно с учетом действующего трудового законодательства.

2. Образовательную деятельность по дополнительным общеобразовательным программам на базе Центра «IT-куб» осуществляют педагоги дополнительного образования. В соответствии с пунктом 4 статьи 46 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» к занятию педагогической деятельностью по дополнительным общеобразовательным программам допускаются лица, обучающиеся по образовательным программам высшего образования по специальностям и направлениям подготовки, соответствующим направленности дополнительных общеобразовательных программ, и успешно прошедшие промежуточную аттестацию не менее чем за два года обучения. Соответствие образовательной программы высшего образования направленности дополнительной общеобразовательной программы определяется образовательной организацией.

2.3 ФОРМЫ АТТЕСТАЦИИ

Формы оценки уровня достижений обучающегося

Для контроля, оценки и самоконтроля эффективности обучения применяются следующие методы:

- **предварительные:** диагностическая анкета, беседа, опрос, наблюдение, выполнение вводных практических заданий;
- **текущие:** педагогическое наблюдение, устный опрос, анализ выполнения практических заданий, решение кейсов и проблемных ситуаций, выполнение интерактивных заданий, участие в играх и групповой работе;
- **промежуточные:** тематические викторины, практические работы, выполнение заданий по разделам программы, анализ цифровых ситуаций;
- **итоговые:** итоговая диагностика, практическое задание по безопасному поведению в цифровой среде, выполнение и защита итогового мини-проекта.

Формы фиксации образовательных результатов

Для фиксации образовательных результатов в рамках курса используются:

- диагностические и проверочные материалы;
- результаты выполнения практических и самостоятельных заданий;
- результаты решения кейсов и ситуационных задач;
- рабочие материалы обучающихся;
- результаты выполнения мини-проектов;
- созданные документы, таблицы и презентации в офисном пакете P7;
- результаты итоговой диагностики;
- листы педагогического наблюдения.

Формы предъявления и демонстрации образовательных результатов

- представление и защита индивидуальных и групповых мини-проектов;
- демонстрация созданных документов и презентаций в Р7;
- решение практических кейсов по кибербезопасности;
- участие в викторинах, интерактивных играх и тематических мероприятиях;
- презентация результатов выполненных практических работ.

Формы подведения итогов реализации программы

- педагогическое наблюдение за динамикой освоения обучающимися содержания программы;
- педагогический анализ выполнения практических и творческих заданий;
- анализ результатов диагностических и проверочных работ;
- оценка самостоятельности обучающихся при выборе безопасной модели поведения в цифровых ситуациях;
- оценка участия обучающихся в групповой и проектной деятельности;
- защита итогового проекта;
- итоговая диагностика уровня сформированности навыков цифровой грамотности и кибербезопасности.

2.4 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Оценивание результатов освоения программы осуществляется на основе критериев, соответствующих возрастным особенностям обучающихся 8–11 лет.

Оцениваемый результат	Высокий уровень	Средний уровень	Недостаточный уровень
Понимание правил безопасного поведения в цифровой среде	Уверенно объясняет основные правила безопасности, самостоятельно применяет их при решении практических ситуаций, может обосновать свой выбор.	Знает основные правила безопасности, применяет их в типичных ситуациях, но иногда нуждается в подсказке.	Знает отдельные правила, затрудняется объяснить их значение и применить в практической ситуации.
Распознавание фишинга и интернет-мошенничества	Самостоятельно выявляет признаки подозрительных сообщений, ссылок и сайтов, объясняет возможные риски и предлагает безопасный алгоритм действий.	Распознаёт основные признаки мошенничества, но при анализе сложных ситуаций нуждается в подсказке.	Не распознаёт основные признаки мошенничества и затрудняется определить безопасный вариант действий.
Защита персональных данных и аккаунтов	Самостоятельно различает персональные и общедоступные сведения, объясняет правила создания надёжных паролей, понимает значение приватности и защиты аккаунта.	Знает основные правила защиты персональных данных и аккаунта, но не всегда самостоятельно применяет их.	Не различает основные виды персональных данных, не понимает необходимости их защиты.

Безопасное поведение в онлайн-играх	Самостоятельно распознаёт опасные ситуации в онлайн-играх, знает способы защиты аккаунта и безопасного общения с незнакомыми игроками, предлагает решения проблемных ситуаций.	Знает основные правила безопасности, но при решении нестандартных ситуаций нуждается в поддержке.	Не распознаёт основные риски онлайн-игр и не знает, как действовать в опасной ситуации.
Безопасное и уважительное онлайн-общение	Соблюдает правила цифрового этикета, уважительно общается, самостоятельно выбирает безопасную модель поведения при возникновении конфликтных ситуаций.	Понимает основные правила общения, но иногда нуждается в напоминании или помощи при решении конфликтных ситуаций.	Имеет существенные пробелы в понимании правил цифрового общения и часто затрудняется выбрать безопасную модель поведения.
Распознавание и противодействие кибербуллингу	Самостоятельно определяет признаки кибербуллинга, знает алгоритм действий, умеет предложить безопасные способы обращения за помощью и поддержки другого человека.	Распознаёт основные признаки кибербуллинга и знает основные способы защиты, но нуждается в подсказке при анализе сложных ситуаций.	Не различает основные формы кибербуллинга и не знает, куда обратиться за помощью.
Определение недостоверной информации и фейков	Самостоятельно выявляет признаки недостоверной информации, использует несколько способов проверки и аргументированно объясняет свой вывод.	Определяет сомнительную информацию с помощью подсказок, знает отдельные способы её проверки.	Не умеет отличать достоверную информацию от недостоверной и не знает способов её проверки.
Оценка надёжности источников информации	Самостоятельно оценивает источник по нескольким критериям, сравнивает источники и объясняет необходимость проверки информации.	Использует отдельные критерии оценки источника, но при анализе нуждается в поддержке.	Не умеет оценивать надёжность источника и не понимает необходимости проверки информации.
Работа с офисным пакетом Р7	Самостоятельно создаёт, редактирует и оформляет документы, таблицы и презентации, соблюдает правила безопасной работы с	Выполняет основные операции в Р7, но испытывает затруднения при использовании отдельных инструментов и	Испытывает значительные трудности при создании и редактировании документов, таблиц и

	файлами и представляет результат.	нуждается в подсказках.	презентаций даже при наличии инструкции.
Применение знаний при решении цифровых ситуаций	Самостоятельно анализирует ситуацию, выявляет возможную угрозу, предлагает несколько вариантов действий и выбирает наиболее безопасный, аргументируя решение.	Правильно определяет основную проблему и выбирает безопасный вариант с помощью подсказки.	Затрудняется определить проблему и выбрать безопасный способ действий.
Проектная деятельность	Самостоятельно планирует работу, выполняет проект, использует цифровые инструменты, представляет результат и отвечает на вопросы.	Выполняет проект по предложенному плану, периодически обращается за помощью, может представить результат.	Испытывает значительные затруднения при выполнении проекта, не соблюдает последовательность работы и нуждается в постоянной помощи.

Шкала оценки уровня освоения компетенций

Механизм оценки уровня освоения компетенции на определённом этапе её формирования строится на основе выделенных критериев и использует пятиуровневую шкалу:

- нулевой уровень — 1 балл;
- низкий уровень — 2 балла;
- средний уровень — 3 балла;
- высокий уровень — 4 балла;
- очень высокий уровень — 5 баллов.

Точкой входа для формирования карты компетенций обучающихся служит **диагностическая анкета (Приложение 1)**.

Итоговая оценка позволяет определить динамику формирования навыков цифровой грамотности, безопасного поведения в сети, критического анализа информации, защиты персональных данных и использования цифровых инструментов.

2.5 МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

При реализации программы используются разнообразные методы и формы организации образовательной деятельности, обеспечивающие сочетание теоретической подготовки с практическим освоением навыков цифровой грамотности и кибербезопасности.

По источнику передачи и восприятия информации:

- **словесные:** объяснение, рассказ, беседа, обсуждение, инструктаж, мини-лекция;
- **наглядные:** демонстрация презентаций, схем, инфографики, учебных скриншотов, примеров цифровых ситуаций, видеоматериалов;
- **практические:** выполнение упражнений, работа с учебными цифровыми материалами, решение кейсов, моделирование ситуаций, создание документов и презентаций.

По характеру познавательной деятельности:

- **объяснительно-иллюстративный:** объяснение нового материала, демонстрация примеров, работа с презентациями и наглядными материалами;
- **репродуктивный:** выполнение заданий по образцу и алгоритму, закрепление правил безопасного поведения;
- **проблемный:** постановка проблемных вопросов, анализ ситуаций, поиск безопасного решения цифровой проблемы;

- **частично-поисковый:** самостоятельный поиск признаков угрозы, сравнение источников, формулирование выводов;
- **исследовательский:** проверка информации, сравнительный анализ сайтов и цифровых сообщений, исследование различных вариантов поведения;
- **проектный:** разработка памяток, презентаций, информационных материалов и итоговых проектов по кибербезопасности;
- **игровой:** дидактические, интерактивные, ролевые, ситуационные и командные игры;
- **кейс-метод:** анализ конкретных или смоделированных цифровых ситуаций и выбор оптимального варианта действий;
- **метод моделирования:** воспроизведение типичных ситуаций онлайн-общения, мошенничества, фишинга, кибербуллинга и других цифровых угроз.

Основные формы организации занятий

- комбинированное занятие;
- практическое занятие;
- занятие-кейс;
- интерактивная игра;
- викторина;
- ролевая игра;
- групповая и командная работа;
- самостоятельная работа;
- проектная работа;
- защита проекта.

Использование данных методов позволяет учитывать возрастные особенности обучающихся 8–11 лет, поддерживать их познавательную активность и формировать не только теоретические знания, но и практические навыки безопасного поведения в цифровой среде.

2.5 МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Наиболее распространено деление методов по:

источнику передачи и восприятия информации:

- ✓ словесный: рассказ, беседа, лекция;
- ✓ наглядный: опыт, иллюстрация, дидактический, наглядный материал, образцы;
- ✓ практический: показ, постановка опытов;

по характеру деятельности:

- ✓ объяснительно-иллюстративный (рассказ, показ, лекция, фильм, карточки и т.п.);
- ✓ репродуктивный (воспроизведение, действие по алгоритму);
- ✓ проблемный (постановка проблемных вопросов, создание проблемных ситуаций);
- ✓ исследовательский метод (опыты, лабораторные, эксперименты, опытническая работа);
- ✓ проектный метод (разработка проектов, моделирование ситуаций, создание творческих работ);
- ✓ метод игры (игры дидактические, развивающие, ролевые, деловые)

3. СПИСОК ЛИТЕРАТУРЫ

Список литературы для педагога:

1. Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник / Е.К. Баранова, А.В. Бабаш. — М.: РИОР: ИНФРА-М, 2019. — 202 с. — (Среднее профессиональное образование)
2. Бирюков А.А. Информационная безопасность защита и нападение: Издательство: ДМК-Пресс, 2018, 474 с.
3. Малых, Т. А. Педагогические условия развития информационной безопасности младшего школьника [Текст]: автореф.дисс. канд. пед. наук Основы безопасности детей и молодежи в Интернете/ Интерактивный курс по интернет – безопасности. –Москва: Иркутск. – 2015. – 56 с.
4. Букина, Е. Ю. Формирование у младших школьников навыков безопасной работы в сети Интернет [Текст] / Е.Ю. Букина // Информатика в школе, Москва, 2014. – № 5 (98). – С. 40–49.
5. Основы кибербезопасности: учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М.: Дрофа, 2019. — 238, [1] с. — (Российский учебник).
6. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы: учеб.пособие для общеобразоват. организаций / М.С. Наместникова. – М.: Просвещение, 2019. – 79 с.: ил. – (Внеурочная деятельность).
7. Цветкова, М.С. Информационная безопасность. Кибербезопасность. 7–9 классы: учебное пособие /М.С. Цветкова, И.Ю. Хлобыстова. — 2-е изд., пересмотр. — М.: БИНОМ. Лаборатория знаний, 2020 — 64 с.: ил.
8. Шаньгин В.Ф. Информационная безопасность и защита информации. / Шаньгин В.Ф. – ДМК-Пресс, 2017 – 702 с.

Список литературы для обучающихся

1. Алигулиев, Р. М. Вопросы защиты детей школьного возраста от интернет-зависимости [Текст] / Р.М. Алигулиев, Р.Ш. Махмудова, Р. Ш. Махмудов. // Дистанционное и виртуальное обучение, Москва, 2011. – № 5. – С. 97–107.
2. Климонтова, Г. Н. Защита информации для современных школьников [Текст] / Г. Н. Климонтова// Воспитательная работа в школе. – 2013. – № 8. – С. 74–81.
3. Никольская К. Значение персональных данных в век информационных технологий // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (4). С. 45-47.

9									
10									
11									
12									

Критерии оценивания

Каждый показатель оценивается по **5-балльной шкале**:

1 балл — нулевой уровень: обучающийся не демонстрирует сформированного навыка, не выполняет задание даже с помощью педагога.

2 балла — низкий уровень: обучающийся выполняет отдельные действия, знает некоторые правила, но испытывает значительные трудности и постоянно нуждается в помощи.

3 балла — средний уровень: обучающийся знает основные правила и выполняет типовые задания, однако в новых или сложных ситуациях нуждается в подсказке.

4 балла — высокий уровень: обучающийся самостоятельно применяет полученные знания, правильно анализирует большинство ситуаций и аргументирует свой выбор.

5 баллов — очень высокий уровень: обучающийся полностью самостоятельно применяет знания в различных ситуациях, умеет объяснить свой выбор, предложить решение и использовать полученные навыки в новой ситуации.

Показатели диагностической карты

1. Безопасное поведение в цифровой среде

Оценивается способность обучающегося соблюдать основные правила безопасного использования компьютера, мобильных устройств, Интернета и цифровых сервисов.

2. Распознавание фишинга и интернет-мошенничества

Оценивается умение находить признаки подозрительных сообщений, ссылок, сайтов и предложений, а также выбирать безопасный алгоритм действий.

3. Защита персональных данных и аккаунтов

Оценивается понимание значения персональных данных, умение соблюдать правила создания надёжных паролей, защиты аккаунтов и сохранения приватности.

4. Безопасное онлайн-общение и кибербуллинг

Оценивается соблюдение правил цифрового этикета, способность распознавать конфликтные и опасные ситуации, связанные с кибербуллингом, и знание способов обращения за помощью.

5. Критическое мышление и проверка информации

Оценивается умение различать факты и мнения, выявлять признаки недостоверной информации, анализировать источник и проверять сведения по нескольким источникам.

6. Работа с офисным пакетом Р7

Оценивается умение создавать и редактировать документы, таблицы и презентации, использовать основные инструменты Р7 и соблюдать правила безопасной работы с файлами.

7. Итоговый проект

Оценивается самостоятельность выполнения проекта, содержание, правильность применения знаний по кибербезопасности, использование цифровых инструментов, представление результата и способность ответить на вопросы.

Расчёт итогового результата

Максимальное количество баллов — 35.

Итоговая сумма	Уровень освоения
1–7 баллов	Нулевой
8–14 баллов	Низкий
15–21 балл	Средний
22–28 баллов	Высокий
29–35 баллов	Очень высокий