

Государственное бюджетное общеобразовательное учреждение
Самарской области средняя общеобразовательная школа с.Узюково
муниципального района Ставропольский Самарской области

РАССМОТРЕНА
На заседании МО
учителей ЕМЦ

СОГЛАСОВАНА
Заместитель
директора по
УВР Дуцева А.Г.

УТВЕРЖДЕНА
Директор ГБОУ СОШ
с.Узюково
Безьянова Т.Ю.
Приказ №77/1-ОД
от «25» августа 2026 г.

РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
(ID 10914290)

Информационная безопасность. Цифровая гигиена
для обучающихся 5-9 классов

с.Узюково 2026

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ОБЩАЯ ХАРАКТЕРИСТИКА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ЦИФРОВАЯ ГИГИЕНА»

Программа направлена на формирование у школьников навыков безопасного и ответственного поведения в цифровой среде. Она учитывает требования ФГОС ООО к предметным (области «Математика и информатика», «Основы безопасности жизнедеятельности»), метапредметным и личностным результатам

Реализация программы обеспечивается нормативными документами:

1. Базовое законодательство и образовательные стандарты

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
- Приказ Минпросвещения России от 31.05.2021 № 287 «Об утверждении федерального государственного образовательного стандарта основного общего образования» (ФГОС ООО).

2. Защита детей и работа с информацией

- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

3. Санитарно-эпидемиологические требования (гигиена цифровой среды)

- СП 2.4.2.4283-26 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодёжи» СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания».
- МР 2.4.0330-23 «Методические рекомендации по обеспечению санитарно-эпидемиологических требований при реализации образовательных программ с применением электронного обучения и дистанционных образовательных технологий».

4. Методические материалы

- Письмо Минобрнауки России от 14.05.2018 № 08-1184 «О направлении информации»
- Письмо Минпросвещения России от 07.06.2019 № 04-474

ЦЕЛИ ИЗУЧЕНИЯ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ЦИФРОВАЯ ГИГИЕНА» - создать условия для профилактики информационных рисков, повысить защищённость учащихся и сформировать культуру информационной безопасности.

Задачи: сформировать навыки работы с цифровой информацией (поиск, анализ, организация, критическое осмысление);развить умения безопасной коммуникации в онлайн-среде; научить распознавать и противостоять различным угрозам (технические, контентные, коммуникационные);способствовать формированию норм информационной этики и права.

МЕСТО КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ЦИФРОВАЯ ГИГИЕНА» В ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Место курса - 34 часа (1 час в неделю). Программу можно реализовать за один учебный год в 5, 7, 8 или 9 классе. Также допустимо распределять разделы последовательно по разным классам или гибко подстраивать под интересы учащихся

ФОРМЫ ПРОВЕДЕНИЯ ЗАНЯТИЙ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ЦИФРОВАЯ ГИГИЕНА»

Использование разнообразных форматов: дискуссии, тренинги (в том числе кейс-метод), практические работы, проектную деятельность, просмотр и обсуждение видеоматериалов

СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

ПЛАНИРУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

Научиться формировать уважительное отношение к окружающим в реальном и виртуальном мире, осознанный и ответственный подход к цифровой активности. уметь ставить цели, выдвигать гипотезы, выбирать способы решения задач; развивать навыки анализа, синтеза, коммуникации.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Умение ставить цели, выдвигать гипотезы, выбирать способы решения задач; развивать навыки анализа, синтеза, коммуникации.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Научиться анализировать доменные имена и адреса в интернете; безопасно использовать средства коммуникации; применять способы самозащиты при попытках мошенничества; организовывать личное цифровое пространство.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/ п	Наименовани е разделов и тем программы	Количеств о часов	Основное содержание	Основные виды деятельности	Электронные (цифровые) образовательные ресурсы
1		34	Баланс развития и безопасности , границы допустимого в цифровом мире	Обсуждение, анализ ситуаций, формулировани е правил	https://cyber-care.ru/lessons/cybersecurity?ysclid=mtfn1w4cg687052146 https://digital-edu.ru/ib7_9 https://урокцифры.рф/lessons/cybersecurity-space?ysclid=mtfn3w41i881779183
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34			

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ (С РАЗДЕЛАМИ)

№ п/ п	Наименование разделов и тем программы	Количес тво часов	Основное содержание	Основные виды деятельности	Электронные (цифровые) образовательные ресурсы
Раздел 1. Информационная безопасность. Цифровая гигиена					
1.1	Цифровая гигиена: зачем это нужно? Понятие периметра безопасности	1	Баланс развития и безопасности, границы допустимого в цифровом мире	Обсуждение, анализ ситуаций, формулирован ие правил	https://ypokцифры.рф/lessons/cybersecurity-space?ysclid=mtfn3w41i881779183
1.2	Общение в социальных сетях и мессенджерах	2	Особенности онлайн- коммуникации, риски	Разбор примеров, обсуждение норм поведения	https://safe.mail.ru/test
1.3	С кем безопасно общаться в интернете	2	Критерии безопасного общения, анализ профилей	Практикум: оценка профилей, выявление рисков	https://prosv.ru/product/informatsionnaya-bezopasnost-kiberbezopasnost-7-9-klass-elektronnaya-forma-uchebnika02/?ysclid=mtfn5w61k38886613

1.4	Персональные данные	2	Что относится к персональным данным, правила их защиты	Составление памятки, разбор кейсов	https://digital-edu.ru/ib7_9
1.5	Настройки конфиденциальности в социальных сетях	3	Как настроить приватность, какие опции использовать	Практическая работа: настройка аккаунта	https://cyber-care.ru/lessons/cybersecurity?ysclid=mtfn1w4cg687052146
1.6	Публикация информации в социальных сетях	2	Риски публикации личных фото и сведений	Анализ примеров, обсуждение последствий	https://урокицифры.рф/lessons/cybersecurity-space?ysclid=mtfn3w41i881779183
1.7	Кибербуллинг и груминг	2	Определение, признаки, способы защиты	Ролевая игра, обсуждение стратегий защиты	https://safe.mail.ru/test
1.8	Фишинг	2	Что такое фишинг, как распознать мошеннические сайты и письма	Тренинг: анализ фишинговых сообщений,	https://wordwall.net/ru/resource/89975396/тренажер-цифровая-гигиена

				правила безопасности	
1.9	Безопасность устройств	3	Что такое вредоносные программы, как они распространяются	Обсуждение, просмотр обучающего видео	https://урокицифры.рф/lessons/cybersecurity-space?ysclid=mtfn3w41i881779183
1.10	Методы защиты от вредоносных программ	2	Антивирус, правила скачивания файлов, осторожность с ссылками	Практикум: проверка файла, обсуждение правил	https://safe.mail.ru/test
1.11	Безопасное использование смартфона или планшета	2	Настройки безопасности, семейный доступ	Практическая работа: настройка устройства	https://prosv.ru/product/informatsionnaya-bezopasnost-kiberbezopasnost-7-9-klass-elektronnaya-forma-uchebnika02/?ysclid=mtfn5w61k38886613
1.12	Резервное копирование данных	2	Зачем нужно резервное копирование,	Практикум: создание	https://digital-edu.ru/ib7_9

			как его организовать	резервной копии	
1.13	Основы государственной политики в области информационной безопасности	2	Основные направления, Доктрина национальной информационно й безопасности	Обсуждение, работа с источниками	https://cyber-care.ru/lessons/cybersecurity?ysclid=mtfn1w4cg687052146
1.14	Подготовка и защита индивидуальных и групповых проектов	3	Выбор темы, сбор информации, презентация результатов	Проектная деятельность: анализ реальной проблемы, поиск решений, защита	https://урокицифры.рф/lessons/cybersecurity-space?ysclid=mtfn3w41i881779183
1.15	Повторение	4	Обобщение изученного, решение практических задач	Ситуационные задачи, тестирование, волонтерская практика (для	https://safe.mail.ru/test

				старших классов)	
Итого		34			
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРАММЕ		34			

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ

№ п/п	Тема урока	Количество часов			Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
1	Цифровая гигиена: зачем это нужно? Понятие периметра безопасности	34	0	32	https://урокцифры.рф/lessons/cybersecurity-space?ysclid=mtfn3w41i881779183
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	0	32	

Методы обучения

- **Объяснительно-иллюстративный.** Базовые понятия (фишинг, социальная инженерия, персональные данные) через лекции, беседы с использованием презентаций, видеоматериалов или инфографики.
- **Проблемный.** Создание на занятиях проблемных ситуаций: «Что делать, если пришло подозрительное письмо?», «Как проверить достоверность новости?».
- **Кейс-метод.** Разбор реальных или смоделированных ситуаций (кейсов): анализ мошеннических схем, случаев кибербуллинга, утечек данных.
- **Практико-ориентированный.** Задания, где нужно применить знания: настроить конфиденциальность в соцсети, создать надёжный пароль, проверить ссылку на безопасность, сделать резервную копию данных.
- **Проектный.** Ученики выполняют проекты: разрабатывают памятку по безопасности, создают инструкцию для младших школьников, готовят презентацию о цифровом следе или цифровой репутации.
- **Игровой.** Для младших школьников особенно эффективны игры: «Цифровой супермаркет» (сортировка контента на полезный и вредный), «Осторожно, фейк!», викторины, ролевые игры (разыгрывание ситуаций общения в сети)
- **Исследовательский.** Небольшие исследования: изучить, какие настройки безопасности есть в популярном сервисе, проанализировать политику конфиденциальности приложения, собрать статистику по распространённым угрозам.

Формы организации деятельности обучающихся

- **Фронтальная (коллективная).** Общие обсуждения, мозговые штурмы, совместные разборы кейсов, подведение итогов.
- **Групповая.** Работа в малых группах (3–5 человек) для анализа темы, подготовки проекта или решения практической задачи.
- **Индивидуальная.** Самостоятельная работа: выполнение практических заданий, подготовка доклада или презентации, рефлексия (например, ведение дневника цифровой гигиены — фиксация ситуаций, где пришлось применить правила безопасности).
- **Смешанная.** Комбинация форм: например, сначала фронтальная беседа, затем групповая работа над кейсом и индивидуальная защита результатов.
- **Дистанционная и смешанная.** Использование электронных курсов, интерактивных симуляторов, образовательных платформ, видеороликов. Это расширяет доступ к материалам и позволяет часть работы вынести на самостоятельную проработку.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Литература

- **Бабаш А. В., Баранова Е. К., Мельников Ю. Н.** «Информационная безопасность: Лабораторный практикум». — М.: КноРус, 2019. — 432 с.

- **Вехов В. Б.** «Компьютерные преступления: способы совершения и раскрытия» / Под ред. акад. Б. П. Смагоринского. — М.: Право и закон, 2014. — 182 с.
- **Громов Ю. Ю., Драчёв В. О., Иванова О. Г.** «Информационная безопасность и защита информации»: Учебное пособие. — Ст. Оскол: ТНТ, 2017. — 384 с.
- **Ефимова Л. Л., Кочерга С. А.** «Информационная безопасность детей. Российский и зарубежный опыт»: Монография. — М.: ЮНИТИ-ДАНА, 2016. — 239 с.
- **Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В.** «Информационная безопасность открытых систем». В 2 т. Т. 2: «Средства защиты в сетях». — М.: ГЛТ, 2018. — 558 с.
- **Наместникова М. С.** «Информационная безопасность, или На расстоянии одного вируса. 7–9 классы. Внеурочная деятельность». — М.: Просвещение, 2019. — 80 с.
- **Кузнецова А. В., Самыгин С. И., Радионов М. В.** «Искусственный интеллект и информационная безопасность общества». — М.: Русайнс, 2017. — 64 с.
- **Солдатова Г. У., Нестик Т. А., Рассказова Е. И., Зотова Е. Ю.** «Цифровая компетентность подростков и родителей. Результаты всероссийского исследования». — М.: Фонд Развития Интернет, 2013. — 144 с.

Информационные ресурсы

- раздел «Защита детей» от «Лаборатории Касперского».
- **detonline.com** — журнал «Дети в информационном обществе»..
- онлайн-курс «Безопасность в Интернете» от Академии Яндекса для школьников 6–9 классов.
- на платформе «Знание. Академия» курс «Цифровая гигиена: как обучать детей безопасности в интернете».