Муниципальное бюджетное общеобразовательное учреждение
«Школа № 74» городского округа Самара

РАССМОТРЕНО	ПРОВЕРЕНО	УТВЕРЖДАЮ
На заседании МО классных руководителей Протокол № 1 от «28» августа 2025г.	Зам. директора по УВ _____И.А. Анненкова «29» августа 2025г.	Директор МБОУ Школа № 74 г.о. Самара _____А.А. Захаркин Приказ № 210-од от 29.08.2025г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 008BDBE3EE3A8FB4AD48A94A017012203C
Владелец: Захаркин Анатолий Александрович
Действителен: с 02.07.2025 до 25.09.2026

Рабочая программа

Курса внеурочной деятельности:

«Информационная безопасность. Цифровая гигиена»

Уровень образования**:** основное общее образование

Составитель: Пивоварова Г.Ф.

Самара,
2025

Пояснительная записка

Рабочая программа внеурочной деятельности «Информационная безопасность. Цифровая гигиена» для 6 класса составлена с учетом требований Федерального закона "Об образовании в РФ" от 29.12.2012 N 273-ФЗ; ФГОС ООО (Приказ №1897 от 17.12.2010г; на основе примерной рабочей программы учебного курса «Цифровая гигиена», рекомендованной координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол №27 от 21.08.2019).

Программа курса «Информационная безопасность. Цифровая гигиена» адресована учащимся 6 классов, а также родителям обучающихся всех возрастов и учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования к предметным (образовательные области «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»), метапредметным и личностным результатам.

Основными целями изучения курса «Информационная безопасность. Цифровая гигиена»являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
- формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информаци-

онных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);

- создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;

- сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;

- сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;

- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Общая характеристика учебного курса

Курс «Цифровая гигиена» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к

обеспечению своей личной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Данный курс предполагает организацию работы в соответствии с содержанием 2-х модулей, предназначенных для обучающихся 6 классов и родителей обучающихся любого возраста соответственно.

Взаимосвязь с программой воспитания

Программа курса внеурочной деятельности разработана с учѐтом федеральных образовательных программ начального общего, основного общего и среднего общего образования. Это позволяет на практике соединить обучающую и воспитательную деятельность педагога, ориентировать еѐ не только на интеллектуальное, но и на нравственное, социальное развитие ребёнка. Это проявляется:

– в выделении в цели программы ценностных приоритетов;

– в приоритете личностных результатов реализации программы внеурочной деятельности, нашедших свое отражение и конкретизацию в программе воспитания;

– в интерактивных формах занятий для обучающихся, обеспечивающих их вовлеченность в совместную с педагогом и сверстниками деятельность.

1. Планируемые результаты

<table>
<tr><td colspan="2">Личностные результаты освоения программы
В результате освоения программы курса «Информационная безопасность. Цифровая гигиена» у обучающихся будут сформированы:
– осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
– готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
– освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
– сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.</td></tr>
<tr><td colspan="2">Предметные результаты освоения программы:</td></tr>
<tr><td>Обучающие научатся:</td><td>– анализировать доменные имена компьютеров и адреса документов в интернете;
– безопасно использовать средства коммуникации,
– безопасно вести и применять способы самозащиты при попытке мошенничества,
– безопасно использовать ресурсы интернета.</td></tr>
<tr><td>Обучающие овладеют:</td><td>– приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.
– использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.</td></tr>
<tr><td>Обучающие получат возможность овладеть:</td><td>– основами соблюдения норм информационной этики и права;
– основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при форми-</td></tr>
</table>

	ровании современной культуры безопасности жизнедеятельности;
Метапредметные результаты освоения программы курса	
Познавательные УУД	В результате освоения учебного курса обучающийся сможет: – выделять явление из общего ряда других явлений; – определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способ-ные быть причиной данного явления, выявлять причины и следствия явле-ний; – строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям; – -мой задачи; – самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации; – критически оценивать содержание и форму текста; – определять необходимые ключевые поисковые слова и запросы.
Регулятивные УУД	В результате освоения учебного курса обучающийся сможет: – идентифицировать собственные проблемы и определять главную проблему; – выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат; – ставить цель деятельности на основе определенной проблемы и существующих возможностей; – выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели; – составлять план решения проблемы (выполнения проекта, проведения исследования); – описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;

Коммуникативные УУД	В результате освоения учебного курса обучающийся сможет: – строить позитивные отношения в процессе учебной и познавательной деятельности; – критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его; – договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей; – делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его. – целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ; – выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации; – использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, со-здание презентаций и др.; – использовать информацию с учетом этических и правовых норм; – создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

1. Содержание курса

№	Название темы	Форма организации	Кол-во часов	Виды деятельности	Содержание
Безопасность общения			***13***		
1	Общение в социальных сетях и мессенджерах	Презентация, беседа	1	– познавательная – проблемно-ценностное общение	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.
2	С кем безопасно общаться в интернете.	Видеоурок, деловая игра	1	– познавательная – игровая	Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.
3	Пароли для аккаунтов социальных сетей.	Видеоурок, беседа	1	– познавательная – проблемно-ценностное общение	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.
4	Безопасный вход в аккаунты.	Презентация, дискуссия	1	– познавательная – проблемно-ценностное общение	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.
5	Настройки конфиденциальности в социальных сетях	Беседа, практическая работа	1	– познавательная – проблемно-ценностное общение	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.
6	Публикация информации в социальных сетях.	Дискуссия, «круглый стол»	1	– познавательная – проблемно-ценностное общение	Персональные данные. Публикация личной информации.

7	Кибербуллинг.	Презентация, дискуссия	1	– познавательная проблемно-ценностное – общение	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.
8	Публичные аккаунты.	Беседа, практическая работа	1	– познавательная – проблемно-ценностное общение	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.
9-10	Фишинг.	Презентация, дискуссия	2	– познавательная – проблемно-ценностное общение	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.
11-13	Выполнение и защита индивидуальных и групповых проектов.	Практическая работа	3	– проблемно-ценностное общение	
Безопасность устройств			***8***		
14	Что такое вредоносный код.	Презентация, дискуссия	1	– познавательная – проблемно-ценностное общение	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.
15	Распространение вредоносного кода.	Видеоурок, интерактивная игра	1	– познавательная – игровая	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.
16-17	Методы защиты от вредоносных программ	Дискуссия, деловая игра	2	– игровая – проблемно-ценностное общение	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.
18	Распространение вредоносного кода для мобильных устройств.	Презентация, дискуссия	1	– познавательная – проблемно-	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

№	Название темы	Форма организации	Кол-во часов	Виды деятельности	Содержание
				ценностное общение	
19-21	Выполнение и защита индивидуальных и групповых проектов.	Практическая работа	3	– проблемно-ценностное общение	
Безопасность информации			***13***		
22	Социальная инженерия: распознать и избежать.	Презентация, беседа	1	– познавательная – проблемно-ценностное общение	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.
23	Ложная информация в Интернете.	«Круглый стол»	1	– проблемно-ценностное общение	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.
24	Безопасность при использовании платежных карт в Интернете.	Презентация, беседа	1	– познавательная	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.
25	Беспроводная технология связи.	Видеоурок, беседа	1	– познавательная – проблемно-ценностное общение	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.
26	Резервное копирование данных.	Беседа, практическая работа	1	– проблемно-ценностное общение	Безопасность личной информации. Создание резервных копий на раз-личных устройствах.
27-28	Основы государственной политики в области формирования культуры информационной безопасности.	Презентация, беседа	2	– познавательная – проблемно-ценностное общение	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.
29-31	Выполнение и защита индивидуальных и	Практическая работа	3	– проблемно-ценностное	

№	Название темы	Форма организации	Кол-во часов	Виды деятельности	Содержание
	групповых проектов.			общение	
32-34	Повторение. Волонтерская практика.		3	– проблемно-ценностное общение	
Количество часов всего			***34***		

2. Тематическое планирование «Информационная безопасность»

№	Название разделов и тем	Количество часов			ЦОР	Форма контроля
		всего	теор.	Практ.		
Первый год обучения						
Безопасность общения		***13***	***7***	***6***		
1	Общение в социальных сетях и мессенджерах	1	1	0		
2	С кем безопасно общаться в интернете.	1	1	0		
3	Пароли для аккаунтов социальных сетей.	1	1	0		Практическая работа
4	Безопасный вход в аккаунты.	1	1	0		
5	Настройки конфиденциальности в социальных	1	0	1		Практическая работа
6	Публикация информации в социальных сетях.	1	0	1		
7	Кибербуллинг.	1	1	0		Тестирование
8	Публичные аккаунты.	1	1	0		
9	Фишинг.	2	1	1		
10	Выполнение и защита индивидуальных и групповых проектов.	3	0	3		Защита индивидуальных проектов

Безопасность устройств		*8*	*4*	*4*		
11	Что такое вредоносный код.	1	1	0		
12	Распространение вредоносного кода.	1	1	0		Практическая работа
13	Методы защиты от вредоносных программ	2	1	1		
14	Распространение вредоносного кода для мобильных устройств.	1	1	0		Тест
15	Выполнение и защита индивидуальных и групповых проектов.	3	0	3		Защита индивидуальных проектов
Безопасность информации		***13***	***5***	***8***		
16	Социальная инженерия: распознать и избежать.	1	1	0		
17	Ложная информация в Интернете.	1	1	0		Практическая работа
18	Безопасность при использовании платежных карт в Интернете.	1	1	0		
19	Беспроводная технология связи.	1	1	0		Тест
20	Резервное копирование данных.	1	0	1		Практическая работа
21	Основы государственной политики в области формирования культуры информационной безопасности.	2	1	1		
22	Выполнение и защита индивидуальных и групповых проектов.	3	0	3		Защита индивидуальных проектов
23	Повторение. Волонтерская практика.	3	0	3		
	Итого	**34**				

Формы контроля:

1. Практическая работа
2. Тестирование
3. Защита индивидуального проекта
4. Форма промежуточной аттестации:Защита 1 проекта

Оценивание: зачет/незачет.

Список литературы:

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К.Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с

2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014. – 182 с.

3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие /Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.

4. Дети в информационном обществе // http://detionline.com/journal/about

5. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт:Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ-ДАНА, 2016. – 239 с.

6. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с.

7. Защита детей by Kaspersky // https://kids.kaspersky.ru/

8. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества /А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017. – 64 с.

9. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.

10. Основы кибербезопасности. // https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa

11. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.

12. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности //Студенческий: электрон. научн. журн. 2019. № 22(66)

13. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144