МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования Самарской области
Юго-Западное управление министерства образования Самарской области
ГБОУ ООШ с. Тяглое Озеро

РАССМОТРЕНО	ПРОВЕРЕНО	УТВЕРЖДЕНО
руководитель МО учителей предметников	и.о. директора по УВР	директор ГБОУ ООШ с. Тяглое Озеро
_____ Федюнина И.Г.	_____ Бочарова В.В.	_____ Федюнина Н.В.
Протокол №1 от «27» августа 2025 г.	Приказ №1 от «28» августа 2025 г.	Приказ № 43/1-од от «29» августа 2025 г.

Федюнина Надежда Викторовна
Digitally signed by Федюнина Надежда Викторовна
Date: 2025.11.17 09:40:54 +04'00'

РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Информационная безопасность

(ID 9589816)

для обучающихся 7 классов

с. Тяглое Озеро, 2025 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ОБЩАЯ ХАРАКТЕРИСТИКА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Программа курса внеурочной деятельности «Информационная безопасность» адресована учащимся 7 классов, 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. Программа курса «Информационная безопасность» разработана на основе программы курса «Информационная безопасность, или на расстоянии одного вируса» Наместниковой М.С.

ЦЕЛИ ИЗУЧЕНИЯ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Основными целями изучения курса 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 информационных объектов с использованием цифровых ресурсов (текстовых, изобрази- тельных, 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.

МЕСТО КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Программа учебного курса «Информационная безопасность» рассчитана на 34 учебных часа, из них 22 часа - учебных занятий, 9 часов - подготовка и защита учебных проектов, 3 часа - повторение. На изучение курса «Информационная безопасность» отводится по 1 часу в неделю в 7 классе.

ФОРМЫ ПРОВЕДЕНИЯ ЗАНЯТИЙ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Формы организации образовательного процесса: поурочная система обучения с использованием объяснительно - иллюстративного, репродуктивного, частично- поискового методов обучения.

СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

7 КЛАСС

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Каждый раздел учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

Раздел 1. «Безопасность общения» Тема 1. Общение в социальных сетях и мессенджерах.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете.

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты .

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях.

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты .

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг.

Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Выполнение и защита индивидуальных и групповых проектов

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода.

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.

Тема 3. Методы защиты от вредоносных программ.

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств.

Расширение вредоносных кодов для мобильных устройств. Правила без- опасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете.

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи.

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности.

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

Выполнение и защита индивидуальных и групповых проектов.

ПЛАНИРУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

В сфере гражданского воспитания курс «Информационная безопасность» может способствовать формированию у учащихся ключевых качеств и навыков, необходимых для осознанного участия в жизни общества. Это достигается через интеграцию гражданско-патриотических, правовых и социальных аспектов в изучение темы информационной безопасности.

Основные направления гражданского воспитания в рамках курса

1. **Формирование правовой культуры и правосознания**
   - Изучение законодательства РФ в сфере защиты информации (например, ФЗ «О персональных данных», «Об информации, информационных технологиях и о защите информации»).
   - Осознание ответственности за нарушение норм информационной этики и права, включая киберпреступления.
   - Развитие навыков соблюдения законов и правил в цифровой среде.
2. **Патриотическое воспитание**
   - Понимание роли информационной безопасности в защите национальных интересов и суверенитета страны.
   - Изучение примеров героических поступков специалистов в области кибербезопасности, связанных с защитой государства.
   - Формирование чувства гордости за достижения российской науки и технологий в сфере информационной безопасности.
3. **Социальная ответственность и гражданская активность**
   - Развитие навыков безопасного поведения в информационном пространстве как части общей социальной ответственности.
   - Участие в проектах и мероприятиях, направленных на повышение информационной грамотности общества (например, проведение уроков безопасности для младших школьников или создание информационных буклетов).
   - Осознание роли каждого гражданина в противодействии информационным угрозам.
4. **Толерантность и межкультурное взаимодействие**
   - Изучение международных стандартов и норм в области информационной безопасности.
   - Развитие навыков критического анализа информации, включая распознавание дезинформации и фейков, которые могут использоваться для разжигания межнациональной розни.

В сфере духовно-нравственного воспитания по курсу «Информационная безопасность»

Формирование нравственного сознания

- Ценностное восприятие информации и информационных технологий через призму духовно-нравственных ориентиров
- Понимание значимости традиционных российских духовно-нравственных ценностей в цифровом пространстве
- Осознание важности этичного поведения в сети Интернет
- Развитие способности различать добро и зло** в информационном пространстве

Развитие морально-этической культуры

- Формирование навыков оценки информации с позиции нравственных норм
- Понимание последствий деструктивного поведения в сети
- Развитие уважения к личности других пользователей
- Осознание ценности человеческого общения в противовес виртуальному

Личностные качества

- Способность противостоять негативному влиянию деструктивного контента
- Развитие критического мышления для распознавания манипулятивных технологий
- Формирование ответственности за свои действия в информационном пространстве
- Развитие эмпатии и умения сопереживать другим пользователям

Планируемые результаты в сфере физического воспитания при изучении курса «Информационная безопасность»

Формирование здорового образа жизни

- Понимание влияния длительного пребывания за компьютером на физическое здоровье
- Освоение принципов эргономичной организации рабочего места
- Формирование привычек регулярных перерывов в работе с техникой
- Осознание важности физической активности при работе с информационными технологиями

Гигиенические навыки

- Соблюдение правил личной гигиены при работе с компьютерной техникой
- Понимание необходимости регулярной уборки рабочего места
- Освоение методов профилактики заболеваний, связанных с длительной работой за компьютером
- Формирование навыков правильного освещения рабочего пространства

Физическое развитие

- Освоение комплексов упражнений для профилактики заболеваний опорно-двигательного аппарата
- Развитие координации движений при работе с компьютерной техникой
- Формирование правильной осанки при работе за компьютером
- Развитие мелкой моторики рук при работе с клавиатурой и мышью
  Профилактические компетенции
- Умение проводить гимнастику для глаз
- Освоение техник снятия мышечного напряжения
- Формирование навыков самоконтроля состояния здоровья при работе с компьютером
- Понимание признаков переутомления и методов его предупреждения

В сфере трудового воспитания при изучении курса «Информационная безопасность»

Профессиональные компетенции

- Освоение базовых навыков работы с информационными технологиями
- Формирование умений эффективного использования цифровых инструментов
- Развитие алгоритмического мышления при решении задач информационной безопасности
- Приобретение опыта проектной деятельности в сфере информационной безопасности

Организационные навыки

- Умение планировать свою работу с информационными ресурсами
- Способность организовывать рабочее пространство для эффективной работы
- Навыки управления временными ресурсами при решении информационных задач
- Формирование культуры систематизации и хранения информации
  Практические умения
- Владение методами защиты информации
- Умение работать с различными программными средствами
- Навыки настройки параметров безопасности устройств
- Способность создавать и поддерживать безопасное информационное пространство

В сфере экологического воспитания при изучении курса «Информационная безопасность»

Понимание экологических взаимосвязей

- Осознание влияния информационных технологий на окружающую среду
- Понимание роли цифровых технологий в решении экологических проблем

- Формирование представлений о взаимосвязи информационной и природной ср еды
- Развитие системного мышления в контексте экологических проблем Экологически ответственное поведение
- Соблюдение принципов ресурсосбережения при работе с техникой
- Формирование навыков рационального использования электронных устройств
- Осознание важности правильной утилизации электронных отходов
- Развитие ответственного отношения к потреблению цифровых ресурсов

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

В сфере овладения универсальными учебными регулятивными действиями.

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 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; оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата; находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата; работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
принимать решение в учебной ситуации и нести за него ответственность.

В сфере овладения универсальными учебными познавательными действиями.

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, способные быть причиной данного явления, выявлять причины и следствия явлений; строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
излагать полученную информацию, интерпретируя ее в контексте решаемой 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.

В сфере овладения универсальными учебными коммуникативными действиями

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.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

7 КЛАСС

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.

приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Обучающийся получит возможность овладеть:

основами соблюдения норм информационной этики и права;

основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;

использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ
7 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов	Основное содержание	Основные виды деятельности	Электронные (цифровые) образовательные ресурсы
1.1	Безопасность общения	13	Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	Беседа, просмотр видеоурока, обсуждение Практическая работа с ресурсами и программами на компьютере	https://урокцифры.рф/lessons/bezopasnost-v-internete-2018-2019
1.2	«Безопасность устройств»	8	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах.	Выявляет и анализирует (при помощи чеклиста) возможные угрозы информационной безопасности объектов.	https://урокцифры.рф/lessons/bezopasnost-budushhego/materials

			Действия при обнаружении вредоносных кодов на устройствах.		
1.3	«Безопасность информации»	13	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы. Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации. Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных	

				аккаунтов.	
Итого		34			
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34			

7 КЛАСС

№ п/п	Тема урока	Количество часов			Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
1	Общение в социальных сетях и мессенджерах	1	0	0	https://digital-likbez.datalesson.ru/videos/8/
2	С кем безопасно общаться в интернете	1	0	0	https://урокцифры.рф/lessons/bezopasnost-v-internete-2018-2019
3	Пароли для аккаунтов социальных сетей	1	0	0	https://урокцифры.рф/lessons/cybersecurity
4	Безопасный вход в аккаунты	1	0	0	https://урокцифры.рф/lessons/cybersecurity
5	Настройки конфиденциальности в социальных сетях	1	0	0	https://resh.edu.ru/page/cyber-project
6	Публикация информации в социальных сетях	1	0	0	https://resh.edu.ru/page/cyber-project
7	Кибербуллинг	1	0	0	https://digital-likbez.datalesson.ru/videos/15/
8	Публичные аккаунты	1	0	0	https://digital-likbez.datalesson.ru/videos/45/
9	Фишинг	2	0	1	https://digital-likbez.datalesson.ru/videos/17/
10	Выполнение и защита индивидуальных и групповых проектов	3	0	1	https://digital-likbez.datalesson.ru

11	Что такое вредоносный код	1	0	0	https://урокцифры.рф/lessons/algoritmy-kod-komanda
12	Распространение вредоносного кода	1	0	0	https://урокцифры.рф/lessons/algoritmy-kod-komanda
13	Методы защиты от вредоносных программ	2	0	0	https://урокцифры.рф/lessons/cybersecurity
14	Распространение вредоносного кода для мобильных устройств	1	0	0	https://урокцифры.рф/lessons/cybersecurity
15	Выполнение и защита индивидуальных и групповых проектов	3	0	1	https://digital-likbez.datalesson.ru
16	Социальная инженерия: распознать и избежать	1	0	0	https://digital-likbez.datalesson.ru/videos/13/
17	Ложная информация в Интернете	1	0	0	https://digital-likbez.datalesson.ru/videos/46/
18	Безопасность при использовании платежных карт в Интернете	1	0	0	https://digital-likbez.datalesson.ru/videos/43/
19	Беспроводная технология связи	1	0	0	https://education.yandex.ru/lab/classes/918380/library/informatics/collection/4info7_2022-23_1hour_prp/?end=2025-11-16&grade=7&group_index=0&module_id=738&start=2025-11-10
20	Резервное копирование данных	1	0	0	https://digital-likbez.datalesson.ru/videos/39/
21	Основы государственной политики в области	2	0	0	https://урокцифры.рф/lessons/clouds-and-ai

	формирования культуры информационной безопасности				
22	Выполнение и защита индивидуальных и групповых проектов	3	0	1	https://урокцифры.рф
23	Повторение	3	0	1	
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	0	5	

8 КЛАСС

№ п/п	Тема урока	Количество часов			Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		0	0	0	

9 КЛАСС

№ п/п	Тема урока	Количество часов			Электронные цифровые образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		0	0	0	