МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

министерство образования Самарской области

Юго-Западное управление

ГБОУ СОШ пос. Ильмень

РАССМОТРЕНО	ПРОВЕРЕНО	УТВЕРЖДЕНО
Рук. ШМО	И.о. зам. директора по УР	Директор
Торгашова К.В.	Культяева Н.Л.	Чуркина Ю.С.
Протокол № 1 от 25.08.2025 г.		Распоряжение № 97-од от 29.08.2025 г.

ЭП

OU=и.о. директора, O=ГБОУ СОШ пос. Ильмень, CN=Чуркина Ю.С., E=ilmen_schpry@samara.edu.ru
00b48a27944f1d471b
2025.09.01 12:30:18+04'00'

РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

(ID 6682446)

«Информационная безопасность»

(ОСНОВНОЕ ОБЩЕЕ ОБРАЗОВАНИЕ)

Ильмень 2025-2026

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ОБЩАЯ ХАРАКТЕРИСТИКА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.

Курс «Информационная безопасность» 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, предназначенного для обучающихся 7 классов.

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей обучающихся 7 классов. Реализации курса осуществляется в рамках внеурочной деятельности обучающихся.

В преподавании модуля «Информационная безопасность» могут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс-методу), дистанционное обучение (электронные курсы, видеоролики, почто- вые рассылки, микрообучение), смешанный формат.

Система учебных заданий должна создавать условия для формирования активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им и профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищенности детей от информационных рисков и угроз (составление памяток, анализ защищенности собственных аккаунтов в социальных сетях и электронных сервисах, практические работы и т.д.).

ЦЕЛИ ИЗУЧЕНИЯ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основными целями изучения курса «Информационная безопасность» 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 Интерне- том.

МЕСТО КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

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

ФОРМЫ ПРОВЕДЕНИЯ ЗАНЯТИЙ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

- беседа;
- практическое занятие;
- защита мини-проекта;
- выступление, доклад, сообщение;

СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 час.

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

Тема 2. С кем безопасно общаться в интернете. 1 час.

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. 1 час.

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

Тема 4. Безопасный вход в аккаунты. 1 час.

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

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.

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

Тема 6. Публикация информации в социальных сетях. 1 час.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 час.

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

Тема 8. Публичные аккаунты. 1 час.

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

Тема 9. Фишинг. 2 часа.

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 проектов3. 3 часа.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

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. 2 час.

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

Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.4

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 1 час.

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

Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.

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

Тема 4. Беспроводная технология связи. 1 час.

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

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 час.

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. 3 часа.5

Повторение. Волонтерская практика. 3 часа.

ПЛАНИРУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

- - 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.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Регулятивные универсальные учебные действия.

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;
- - 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.

Познавательные универсальные учебные действия.

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.

Коммуникативные универсальные учебные действия.

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, создание 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.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Выпускник научится:

- - 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.

Выпускник овладеет:

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

Выпускник 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.

7 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов	Основное содержание	Основные виды деятельности	Электронные (цифровые) образовательные ресурсы
1	Безопасность общения	13	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент. Персональные данные как основной капитал личного пространства в цифровом мире. Правила	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет. Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения. Изучает основные понятия регистрационной информации и шифрования. Умеет их	**Библиотека цифрового образовательного контента** https://academy-content.apkpro.ru/ru/search?term=информационная%20безопасность%207%20класс

			добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	применить. Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа. Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле. Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач. Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников. Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила	

			Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах. Персональные данные. Публикация личной информации. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	информационной безопасности. Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу	

			Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг. Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.		
2	Безопасность	8	Виды вредоносных кодов.	Соблюдает технику безопасности при	**Библиотека цифрового образовательного**

	устройств		Возможности и деструктивные функции вредоносных кодов. 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.	эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче. Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов. Изучает виды антивирусных программ и правила их установки. Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся младшего возраста. Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы,	**контента** https://academy-content.apkpro.ru/ru/search?term=информационная%20безопасность%207%20класс

			Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов. Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	аксиомы, теории.	
3	Безопасность информации	13	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска. Определяет возможные источники	**Библиотека цифрового образовательного контента** https://academy-content.apkpro.ru/ru/search?term=информационная%20безопасность%207%20класс

			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. Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в	необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации. Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете. Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов. Создает резервные копии. Умеет привести выдержки из законодательства РФ:	

			публичных сетях. Безопасность личной информации. Создание резервных копий на различных устройствах. Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной	• обеспечивающего конституционное право на поиск, получение и распространение информации; • отражающего правовые аспекты защиты киберпространства	

			безопасности		
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34			