МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования Самарской области
Юго - Западное управление министерства образования Самарской области
ГБОУ СОШ пос. Прибой

РАССМОТРЕНО	ПРОВЕРЕНО	УТВЕРЖДЕНО
Руководитель МО	и.о. заместитель директора по УВР	Директор
_____Тагдирова Ю.С.	_____Юркив А.А.	_____Пономаренко И.В.
Протокол №1	«29» августа 2025 г.	Приказ №70
от «29» августа 2025 г.		от «29» августа 2025 г.

ЭП
Пономаренко И.В.
C=RU, OU=Директор, O=ГБОУ СОШ пос. Прибой, CN=Пономаренко И.В., E=riboy_sch_bzn@63edu.ru
я подтверждаю этот документ
2025-09-02 09:47:14

РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

(ID 8373399)

Информационная безопасность

для обучающихся 7 класса

п. Прибой, 2025

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ОБЩАЯ ХАРАКТЕРИСТИКА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «Информационная безопасность»

Курс внеурочной деятельности «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.

ЦЕЛИ ИЗУЧЕНИЯ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «Информационная безопасность»

- формирование активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им;
- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз.

МЕСТО КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «Информационная безопасность» В ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Курс внеурочной деятельности «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. Данный курс предполагает изучение Модуля 1 (для обучающихся) авторской программы «Информационная», разработанной Наместниковой М.С., в течение одного года для обучающихся 7-8 классов.

ФОРМЫ ПРОВЕДЕНИЯ ЗАНЯТИЙ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «Информационная безопасность»

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

СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
«Информационная безопасность»
7 КЛАСС

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

Каждый раздел курса внеурочной деятельности завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста. За счет часов, предусмотренных для повторения материала (4 часа), возможно проведение занятий для учащихся 4-6 классов. Эти занятия в качестве волонтерской практики могут быть проведены учащимися. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайн занятия, подготовленные входе выполнения учебных заданий по основным темам курса.

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 проектов 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 часа

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

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

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
7 КЛАСС
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 данных.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ
7 КЛАСС

№ п/п	Наименование разделов и тем программы	Количество часов	Основное содержание	Основные виды деятельности	Электронные (цифровые) образовательные ресурсы
**«Информационная безопасность» **					
Раздел 1. **«Информационная безопасность» **					
1.1	Тема 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 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. Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и	Соблюдает технику безопасности при 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 более младшего возраста. Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает	

			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. 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.	в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории. Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.	
1.2	Тема 2. «Безопасность устройств»	8	Виды вредоносных кодов. 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. Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов. Расширение вредоносных кодов для мобильных	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 применить. Объясняет причины использования безопасного входа при работе на	

			устройств. Правила безопасности при установке приложений на мобильные устройства.	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 информационной безопасности. Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек листа (памятки) по противодействию фишингу. Самостоятельная работа.	
1.3	Тема 3 «Безопасность информации»	13	Приемы социальной инженерии. Правила безопасности при виртуальных контактах. Цифровое пространство как площадка самопрезентации, экспериментирования и освоения	Находит нужную информацию в базах данных, составляя запросы на поиск.Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить	

			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 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 безопасности.	источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете. Систематизирует получаемую информацию в процессе поиска. Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации. Создает резервные копии. Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации; - отражающего правовые аспекты защиты киберпространства. Самостоятельная и групповая работа по созданию продукта проекта	
Итого		34			

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ
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			
2	С кем безопасно общаться в интернете	1			
3	Пароли для аккаунтов социальных сетей	1			
4	Безопасный вход в аккаунты	1			
5	Настройки конфиденциальности в социальных сетях	1			
6	Публикация информации в социальных сетях	1			
7	Кибербуллинг	1			
8	Публичные аккаунты	1			
9	Фишинг	2			
10	Выполнение и защита индивидуальных и групповых проектов	3			
11	Что такое вредоносный код?	1			
12	Распространение вредоносного кода	1			
13	Методы защиты от вредоносных программ	2			
14	Распространение вредоносного кода для мобильных устройств	1			
15	Выполнение и защита индивидуальных и групповых проектов	3			
16	Социальная инженерия: распознать и	1			

	избежать				
17	Ложная информация в Интернете	1			
18	Безопасность при использовании платежных карт в Интернете	1			
19	Беспроводная технология связи	1			
20	Резервное копирование данных	1			
21	Основы государственной политики в области формирования культуры информационной безопасности	2			
22	Выполнение и защита индивидуальных и групповых проектов	3			
23	Повторение, волонтерская практика, резерв	3			
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		34	0	0	