

Муниципальное бюджетное общеобразовательное учреждение городского округа Тольятти «Школа №80 имени Героя Муниципальное бюджетное общеобразовательное учреждение городского округа Тольятти «Школа №80 имени Героя Социалистического Труда А.С. Мурысева» (МБУ «Школа № 80»)

Программа рассмотрена

Согласовано

Утверждаю

на заседании МО классных

Зам. директора по УВР

Директор

руководителей

Рожкова Н.Э

Н.А. Кирсанова

Протокол № 1

«29» 08. 2025 г.

«29» 08. 2025г. пр. № 130/ОД

Затолокина Т.В

от «27» 08. 2025г.

Рабочая программа по внеурочной деятельности

«Информационная безопасность»

## Пояснительная записка

Программа разработана на основе: федерального государственного образовательного стандарта основного общего образования по предметным образовательным областям «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности»; Учебного плана внеурочной деятельности МБУ «Школа №80»;

Примерной рабочей программы учебного курса «Цифровая гигиена» основного общего образования, рекомендованного Координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019);

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, 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 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.

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 курса внеурочной деятельности «Информационная безопасность» отводится 1 час в неделю в 7 классе

## Личностные, метапредметные и предметные результаты освоения учебного курса

### Предметные:

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.

#### Метапредметные

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.

#### Личностные

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.

## Содержание программы

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 в ходе 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. 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 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. 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 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

### Тематическое планирование

курса внеурочной деятельности «Информационная безопасность»

№ п/п	Тема	Кол- во часов	Пр им ер ны е сро ки пр ове де ни я	Основное содержание	Характеристика основных видов учебной деятельности обучающихся

Тема 1. «Безопасность общения»

1	Общение в социальных сетях мессенджерах	1		Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	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.
2	С кем безопасно общаться в интернете	1		Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.
3	Пароли для аккаунтов социальных сетей	1		Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.

4	Безопасный вход в аккаунты	1		Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.
5	Настройки конфиденциальности в социальных сетях	1		Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.
6	Публикация информации в социальных сетях	1		Персональные данные. Публикация личной информации.	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.
7	Кибербуллинг	1		Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Публичные аккаунты	1		Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
9	Фишинг	2		Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу.
10	Выполнение и защита индивидуальных и групповых проектов	3			Самостоятельная работа.

Тема 2. «Безопасность устройств»

1	Что такое вредоносный код?	1		Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.
---	----------------------------	---	--	--	--

2	Распространение вредоносного кода	1		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.	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.
3	Методы защиты от вредоносных программ	2		Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	Изучает виды антивирусных программ и правила их установки.
4	Распространение вредоносного кода для мобильных устройств	1		Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.
5	Выполнение и защита индивидуальных и групповых проектов	3			Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.

### Тема 3 «Безопасность информации»

1	Социальная инженерия: распознать и избежать	1		Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
2	Ложная информация в Интернете	1		Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.

3	Безопасность при использовании платежных карт в Интернете	1		Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	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.
4	Беспроводная технология связи	1		Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
5	Резервное копирование данных	1		Безопасность личной информации. Создание резервных копий на различных устройствах.	Создает резервные копии.
6	Основы государственной политики в области формирования культуры информационной безопасности	2		Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.	Умеет привести выдержки из законодательства РФ: обеспечивающего конституционное право на поиск, получение и распространение информации; отражающего правовые аспекты защиты киберпространства.
7	Выполнение и защита индивидуальных и групповых проектов	3			Самостоятельная и групповая работа по созданию продукта проекта
8	Повторение, волонтерская практика, резерв	3			
Итого:		34 часа			

Требования к содержанию итоговых проектно-исследовательских работ

Критерии содержания текста проектно-исследовательской работы

Во введении сформулирована актуальность (личностная и социальная значимость) выбранной проблемы. Тема может быть переформулирована, но при этом четко определена, в необходимости исследования есть аргументы.

Правильно составлен научный аппарат работы: точность формулировки проблемы, четкость и конкретность в постановке цели и задач, определении объекта и предмета исследования, выдвижении гипотезы. Гипотеза сформулирована корректно и соответствуют теме работы.

Есть планирование проектно-исследовательской деятельности, корректировка ее в зависимости от результатов, получаемых

на разных этапах развития проекта. Дана характеристика каждого этапа реализации

проекта, сформулированы задачи, которые решаются на каждом этапе, в случае коллективного проекта – распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведен корректно.

Используется и осмысливается междисциплинарный подход к исследованию и проектированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников.

Определён объём собственных данных и сопоставлено собственное проектное решение с аналоговыми по проблеме. Дан анализ источников и аналогов с точки зрения значимости для собственной проектно-

Исследовательской работы, выявлена его новизна, библиография и интернет ресурсы грамотно оформлены.

Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.

Есть оценка результативности проекта, соотнесение с поставленными задачами. Проведена оценка социокультурных и образовательных последствий проекта на индивидуальном и общественном уровнях.

Критерии презентации проектно-исследовательской работы (устного выступления).

Демонстрация коммуникативных навыков при защите работы. Владение риторическими умениями, раскрытие автором содержания работы, достаточная осведомленность в терминологической системе проблемы, отсутствие стилистических и речевых ошибок, соблюдение регламента.

Умение чётко отвечать на вопросы после презентации работы.

Умение создать качественную презентацию. Демонстрация умения использовать ИТ-технологии и создавать слайд презентацию на соответствующем его возрасту уровне.

Умение оформлять качественный презентационный буклет на соответствующем его возрасту уровне.

Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видео-ролик, мультфильм и т.д.).

Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации коммуникабельности, благодарности и уважения по отношению к руководителю, консультантам, умение четко обозначить пути создания сетевого продукта.

Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.

## Список литературы

- Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с
- 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.
- 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.
- Дети в информационном обществе // <http://detionline.com/journal/about>
- Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИДАНА, 2016. – 239 с.
- 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.
- Защита детей by Kaspersky // <https://kids.kaspersky.ru/>
- Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017. – 64 с.
- Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.
- Основы кибербезопасности. // <https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa>
- Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.
- Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон. научн. журн. 2019. № 22(66)
- 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 с.