

**Муниципальное автономное общеобразовательное учреждение
средняя общеобразовательная школа №2 имени Ж.И.Алфёрова**

ПРИНЯТО
на заседании
педагогического
совета протокол
от «29» 08 2025 г.
№ 01

УТВЕРЖДЕНО
приказом
от «01» 09 2025 г.
№ 142
директора МАОУ
_____ Е.В.Медведева

Подписано цифровой подписью: Медведева Елена Владимировна
DN: E=uc_fk@roskazna.ru, S=77 Москва, ИИН
ЮЛ=7710568760, ОГРН=1047797019830,
STREET="Большой Златоустинский переулок, д. 6, строение 1",
L=г. Москва, C=RU, O=Казначейство России, CN=Казначейство
России
Причина: Я утвердил этот документ
Дата: 01 Сентябрь 2025 г. 12:22:10

**РАБОЧАЯ ПРОГРАММА ПО ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

7 - 9 классы (ФГОС ООО)
(социальное направление)

г. Туринск
2025

Пояснительная записка

Настоящая программа внеурочной деятельности «Информационная безопасность» в 7-9 классах написана на основании следующих нормативных документов:

- Федерального Государственного Образовательного Стандарта (ФГОС), утвержденного приказом Министерством образования и науки Российской Федерации от 17 декабря 2010 г. № 1897;
- авторской программы «Информационная безопасность или на расстоянии одного вируса» разработанной Наместниковой М.С.

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:

1. 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);
2. 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;
3. 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.;
4. 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;
5. сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

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.

Место курса в учебном плане: 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 по 1 часу в неделю в 7, 8, 9 классах.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ

Предметные:

В результате изучения курса учащиеся смогут:

- 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.

Учащийся овладеет:

- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.;
- 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; правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

СОДЕРЖАНИЕ КУРСА

7 класс

Раздел 1. «Безопасность общения» - 13 ч.

Общение в социальных сетях и мессенджерах. С кем безопасно общаться в интернете. Пароли для аккаунтов социальных сетей. Безопасный вход в аккаунты. Настройки конфиденциальности в социальных сетях. Публикация информации в социальных сетях. Кибербуллинг. Публичные аккаунты. Фишинг. Выполнение и защита групповых проектов.

Раздел 2. «Безопасность устройств» - 8 ч.

Что такое вредоносный код? Распространение вредоносного кода. Методы защиты от вредоносных программ. Распространение вредоносного кода для мобильных устройств. Выполнение и защита групповых проектов.

Раздел 3. «Безопасность информации» - 13 ч.

Социальная инженерия: распознать и избежать. Ложная информация в Интернете. Безопасность при использовании платежных карт в Интернете. Беспроводная технология связи. Резервное копирование данных. Основы государственной политики в области формирования культуры информационной безопасности. Выполнение и защита групповых проектов. Повторение. Волонтерская практика.

8 класс

Раздел 1. «Общие сведения о безопасности ПК и Интернета» - 5 ч.

Как устроены компьютер и Интернет. Как работают мобильные устройства. Угрозы для мобильных устройств. Защита персональных данных. Компьютерная и информационная безопасность. Основные угрозы безопасности информации. ПР №1 «Создание газеты «Безопасность в Интернете».

Раздел 2. «Техника безопасности и экология» - 5 ч.

Правила поведения в компьютерном кабинете. Компьютер и мобильные устройства в чрезвычайных ситуациях. Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду. Комплекс упражнений при работе за компьютером. Гигиена при работе с ПК. ПР №2 «Создание буклета «Техника безопасности при работе с компьютером».

Раздел 3. «Проблемы Интернет-зависимости» - 5 ч.

ЗОЖ и компьютер. Деструктивная информация в Интернете. Как ее избежать. Психологическое воздействие информации на человека. Управление личностью через сеть Интернет и компьютер зависимость (аддикция). Как развивается зависимость. Типы интернет – зависимости. ПР №3 «Создание мультимедийной презентации «ПК и ЗОЖ. Организация рабочего места».

Раздел 4. «Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы» - 5 ч.

Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов. Отличия вирусов и закладок. Как распространяются вирусы. ПР №4 «Создание презентации на тему «Разновидности вирусов. Черви, трояны, скрипты». Что такое антивирусная защита. Как лечить компьютер? Антивирусные программы для ПК. Выявление неизвестных вирусов. ПР №5 «Установка антивирусной программы». Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.

Раздел 5. «Мошеннические действия в Интернете. Киберпреступления» - 5 ч.

Виды интернет – мошенничества. Мошеннические действия в сети. Предложения о разблокировании программ. Ложные антивирусы. «Легкий» заработок в Интернете. Мошенничество при распространении «бесплатного» ПО. Азартные игры. Онлайн-казино. Технологии манипулирования в Интернете. Техника безопасности при интернет-общении. ПР №6 «Доклад на тему: «Правила поведения в сети с мошенниками и злоумышленниками».

Раздел 6. «Сетевой этикет. Психология и сеть» - 5 ч.

Что такое этикет. Виды этикета. Сетевой этикет. Общие правила сетевого этикета. Этикет и безопасность. Безопасная работа в сети в процессе сетевой коммуникации. Психологическая обстановка в Интернете. Если вы стали жертвой компьютерной. Агрессии. ПР №7 «Выпуск видеоролика на тему «Как не испортить себе настроение при общении в Сети и не

опуститься до уровня «веб-агрессора».

Раздел 7. «Государственная политика в области кибербезопасности» - 4 ч.

Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация. Защита прав потребителей при использовании услуг Интернет. Как расследуются преступления в сети. Ответственность за интернет-мошенничество. ПР №8 «Создание презентации «Как уберечь свою персональную информацию в Интернете, если вы общаетесь в социальных сетях».

9 класс

Социальная инженерия: распознать и избежать. Ложная информация в Интернете. Безопасность при использовании платежных карт в Интернете. Беспроводная технология связи. Резервное копирование данных. Подготовка к итоговому тесту. Выполнение теста Обсуждение тем групповых проектов. Выполнение и защита групповых проектов. Повторение.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

7 класс

№	Раздел	Кол-во часов	Образовательные ресурсы, включая электронные
1	Безопасность общения	13	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
2	Безопасность устройств	8	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://resh.edu.ru
3	Безопасность информации	13	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
Итого:		34	

8 класс

№	Раздел	Кол-во часов	Образовательные ресурсы, включая электронные
1	Общие сведения о безопасности ПК и Интернета	5	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
2	Техника безопасности и экологии	5	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://resh.edu.ru
3	Проблемы Интернет-зависимости	5	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://resh.edu.ru
4	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	5	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
5	Мошеннические действия в Интернете. Киберпреступления.	5	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
			https://resh.edu.ru
6	Сетевой этикет. Психология и сеть.	5	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
7	Государственная политика в области кибербезопасности.	4	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://resh.edu.ru
Итого:		34	

9 класс

№	Раздел	Кол-во часов	Образовательные ресурсы, включая электронные
1	Социальная инженерия: распознать и избежать	4	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
2	Ложная информация в Интернете	6	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
3	Безопасность при использовании платежных карт в Интернете	4	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
4	Беспроводная технология связи	4	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
5	Резервное копирование данных	4	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
6	Подготовка к итоговому тесту	1	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
			https://resh.edu.ru
7	Выполнение теста	1	
8	Обсуждение тем групповых проектов	2	
9	Выполнение и защита групповых проектов.	4	
10	Повторение.	4	https://bosova.ru/metodist/authors/informatika/3/eor10.php https://intuit.ru/studies/courses/10/10/info https://resh.edu.ru
Итого:		34	

