



Муниципальное бюджетное образовательное учреждение
«Средняя общеобразовательная школа № 3»
муниципального образования «город Бугуруслан»

«Рассмотрено»
на педагогическом совете
Протокол №1
от «31» августа 2023г.

«Согласовано»
заместитель директора по ВР
Е.В. Афонина
«31» августа 2023г.

«Утверждено»
МБОУ СОШ № 3
Е.В. Кручинкина
Приказ №99 от 31.08.2023г.



Рабочая программа внеурочной деятельности

«Цифровая безопасность»

Возраст обучающихся: 14 лет

Срок реализации: 1 год

Авт.-сост.: Ильц Д.А.

Реализует: Ильц Д.А, учитель начальных
классов

2023 – 2024 учебный год

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Курс «Цифровая 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.

Основными **целями** изучения курса «Цифровая 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.

Общая характеристика учебного курса

Курс внеурочной деятельности «Цифровая 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. На изучение курса внеурочной деятельности «Цифровая безопасность» отводится по 1 часу в неделю 8 классах.

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, интернетсервисов 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 цифровой безопасности.

Содержание программы

Раздел 1. «Общие сведения о безопасности ПК и интернета»

Тема 1. Как устроен компьютер и Интернет. 1 час.

Базовые операции при использовании мессенджеров и социальных сетей. История и социальная значимость личных аккаунтов в сети Интернет.

Тема 2. Как работают мобильные устройства. Угрозы для мобильных устройств.

Раздел 2. «Техника безопасности и экология»

Тема 1. Компьютер и мобильные устройства в чрезвычайных ситуациях. 1 час

Опасные ситуации, провокации и попытки манипуляции со стороны виртуальных собеседников.

Тема 2. Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду. 1 час

Источники информации разного типа и для разных аудиторий, соблюдение правил информационной безопасности

Тема 3. Создание буклета «Техника безопасности при работе с компьютером». 1 час

Самостоятельная работа.

Раздел 3. «Проблемы Интернет - зависимости»

Тема 1. ЗОЖ и компьютер. Деструктивная информация в интернете, как ее избежать. 1 час.

Техника безопасности при эксплуатации компьютерных систем.

Тема 2. Психологическое воздействие информации на человека. 1 час

Информационное воздействие, которое создает угрозу для развития личности и отстраняет индивида от социума, создает дефицит живого общения.

Тема 3. Интернет и компьютерная зависимость. 1 час

Что такое зависимость. Виды и причины зависимостей.

Раздел 4. «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. 2 часа

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.

Раздел 5. «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.

Раздел 6. «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.

Тема 7. Выполнение теста. 1 час

Самостоятельная работа.

Тема 8. Обсуждение тем индивидуальных рефератов. 1 час

Тема 9. Защита рефератов. 3 час.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Тема	Количество часов	Характеристика основных видов деятельности
Раздел 1. «Общие сведения о безопасности ПК и Интернета»			
1	Как устроен компьютер и Интернет.	1	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	Как работают мобильные устройства. Угрозы для мобильных устройств	1	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.
Раздел 2. «Техника безопасности и экология»			
3	Компьютер и мобильные устройства в чрезвычайных ситуациях	1	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
4	Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду	1	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
5	«Создание буклета «Техника безопасности при работе с компьютером»	1	Самостоятельная работа.
Раздел 3. «Проблемы Интернет - зависимости»			
6	ЗОЖ и компьютер. Деструктивная информация в в интернете, как ее избежать.	1	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.
7	Психологическое воздействие информации на человека. Управление личностью через сеть.	1	Информационное воздействие, которое создает угрозу для развития личности и отстраняет индивида от социума, создает дефицит живого общения.
8	Интернет и компьютер зависимость.	1	Виды и причины зависимостей.
Раздел 4. «Безопасность общения»			
9	Общение в социальных сетях и мессенджерах	1	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.

10	С кем безопасно общаться в интернете	1	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.
11	Пароли для аккаунтов социальных сетей	1	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.
12	Безопасный вход в аккаунты	1	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.
13	Настройки конфиденциальности в социальных сетях	1	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.
14	Публикация информации в социальных сетях	1	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.
15	Кибербуллинг	1	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
16	Публичные аккаунты	1	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
17	Фишинг	2	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу.

Раздел 5. «Безопасность устройств»

18	Что такое вредоносный код?	1	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.
19	Распространение вредоносного кода	1	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.
20	Методы защиты от вредоносных программ	2	Изучает виды антивирусных программ и правила их установки.

Раздел 6. «Безопасность информации»

21	Социальная инженерия: распознать и избежать	1	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
22	Ложная информация в Интернете	1	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает
23	Безопасность при использовании платежных карт в Интернете	1	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.
24	Беспроводная технология связи	1	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.

25	Резервное копирование данных	1	Создает резервные копии.
26	Основы государственной политики в области формирования культуры информационной безопасности	2	Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации;
27	Выполнение теста	1	Самостоятельная работа
28	Обсуждение тем индивидуальных рефератов	1	Обсуждение
29	Защита рефератов	3	Защита рефератов
Итого:		34ч.	

Список литературы.

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2016. — 136 с.
2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.
3. 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.
4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ- ДАНА, 2016. — 239 с.
5. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2016. — 239 с.
6. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г. Милославская. — М.: ГЛТ, 2017. — 536 с.
7. 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.
8. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.
9. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 с.
10. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинкова, В.В. Гафнер. — М.: АРТА, 2016. — 296 с.
11. Семенов, В.А. Информационная безопасность: Учебное пособие / В.А. Семенов. — М.: МГИУ, 2017. — 277 с.
12. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 366с.

