государственное бюджетное общеобразовательное учреждение Самарской области «Школа-интернат для обучающихся с ограниченными возможностями здоровья с. Обшаровка Приволжского района Самарской области»

Адрес: 445550, Самарская область, Приволжский район, с. Обшаровка, ул. Советская, 98, Телефон (факс): (84647) 93236, mail: gscou_prv@63edu.ru

Рассмотрено на заседании методического объединения 25.08.2025 г.	Проверено И.о. заместителя директора по УВР _____О. Н. Никитина	«Утверждаю» Директор ГБОУ школы-интерната с. Обшаровка _____ Н.В.Шабашева Приказ № 340 от 26.08.2025г.

Программа кружковой деятельности

по курсу «Цифровая гигиена»

предметная область

«Внеурочная деятельность»

1 вариант

6-9 классы

CN=Н.В. Шабашева, O=ГБОУ школа-интернат с. Обшаровка, OU="", E=gscou_prv@63edu.ru, C=RU
00c4cd8932c4ba0f9f
2025.09.16 13:40:40+04'00'

Составитель программы:
Рафейчик Ольга Александровна,
учитель высшей квалификационной категории

Обшаровка, 2025г.

1. Пояснительная записка

Программа кружковой деятельности по курсу «Цифровая гигиена» (далее — программа) представляет учащемся с интеллектуальными нарушениями возможность овладеть базовыми навыками безопасной работы с интернетом.

Данная программа создает условия для развития у обучающихся теоретических и практических знаний компьютерной грамотности, формирования информационно-коммуникативных знаний и умений. В результате этих занятий учащиеся достигают значительных успехов в своем развитии, овладевают безопасными приемами работы в сети интернет.

Отличительные особенности программы заключаются в том, что она разработана с учетом психофизических особенностей учащихся с нарушением интеллекта. Программа включает в себя коррекционные упражнения и задания, которые позволяют учащимся с интеллектуальными нарушениями освоить программу.

В данной программе применяются следующие технологии: проектная деятельность, модульное обучение, которые позволяют сделать обучение индивидуализированным, доступным, вариативным; используемые формы (средства, методы) образовательной деятельности позволяют достичь поставленную цель путем адаптированных форм и методов работы.

Цель программы: освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства.

Для успешной реализации поставленной цели необходимо решить следующие *задачи*:

- обучающие:
  - расширить, актуализировать знания о назначении социальных сетей и мессенджеров;
  - закрепить правила безопасности при установке приложений на мобильные устройства;

— создать условия для получения обучающимися практических знаний и умений;
— мотивировать обучающихся к самостоятельному изучению поиска в интернете по заданной теме;
— стимулировать обучающихся к самостоятельному поиску необходимой информации;
— сформировать у обучающихся потребность в культуре поведения в интернет сообществах;
— закрепить в самостоятельной деятельности умение применять полученные знания на практике;
— дать возможность применить на практике полученные знания о создании своей странички и паролей;
— содействовать усвоению (овладению) компьютерной терминологии;

- развивающие:
  — развивать коммуникативные навыки;
  — развивать умение обрабатывать полученную информацию;
  — развивать познавательный интерес к детским обучающим платформам;
  — развивать самостоятельность при создании своей странички и паролей сайта;
  — формировать умение работать по алгоритму;
  — способствовать развитию логического мышления, пространственного воображения, памяти, наблюдательности, умения правильно обобщать данные и делать выводы, сравнивать, умения составлять план и пользоваться им и т.д.;
  — развивать умение высказывать свою точку зрения о проделанной работе;
- воспитательные:
  — содействовать воспитанию усидчивости и настойчивости в работе;
  — воспитывать умение доводить начатое дело до конца;
  — обеспечить элементарную творческую активность при выполнении

практических заданий;

— создать условия, обеспечивающие воспитание целеустремленности;

— воспитывать уважение к своим товарищам в группе;

— формировать ценностные ориентиры на безопасное и здоровое общение в сети интернет.

Программа «Цифровая гигиена» адресована обучающимся 6-9 классов. Данная возрастная категория характеризуется стремлением к познанию новой информации и самостоятельным решениям, что позволяет использовать в программе технологии проблемных ситуаций и проектной деятельности.

Набор в группы осуществляется на добровольной основе, то есть принимаются все желающие заниматься (в случае наличия плохого зрения у обучающихся, необходима справка медицинского осмотра и допуска к занятиям).

Программа рассчитана на 1 год обучения, всего 34 часа в год.

Формы организации деятельности: индивидуально-групповая.

Формы обучения: используются теоретические, практические, комбинированные.

Виды занятий по программе определяются содержанием программы и предусматривают: беседы, игры, самостоятельную работу, участие в интернет-олимпиадах и интернет-уроках.

Занятия по программе «Цифровая гигиена» проводятся раз в неделю. Исходя из санитарно-гигиенических норм, продолжительность часа занятий для учащихся составляет 25 минут теоретической деятельности, 25 минут практической деятельности с перерывами на разминку для глаз и двигательную паузу.

2. Содержание программы

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных

сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 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. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг. Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься отфишеров в социальных сетях и мессенджерах. Выполнение и защита индивидуальных и групповых проектов.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. Виды вредоносных кодов.

Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 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. Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств. Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Тема 5. Выполнение и защита индивидуальных и групповых проектов.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете. Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи. Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных. Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 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 и защита индивидуальных и групповых проектов.

3. Планируемые результаты

Личностные:

- вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;
- формируются и развиваются нравственные, этические, патриотические качества личности;
- стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

Предметные:

обучающиеся научатся:

- 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;

овладеют:

- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.
- использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных;
- использовать приемы работы с антивирусными программами, запускать программы-антивируса для сканирования компьютера и внешних носителей информации, устанавливать и сканировать антивирусной программой;
- дозировано использовать личную информацию в сети интернет; различать (распознавать) мошеннические действия;

- корректно общаться в сети Интернет.

Уровни освоения	Результат
Достаточный	Учащиеся демонстрируют заинтересованность в учебной, познавательной и творческой деятельности, составляющей содержание программы. На итоговой работе показывают удовлетворительное знание теоретического материала, практическое применение знаний воплощается в качественный продукт, без руководящей помощи педагога.
Минимальный	Учащиеся демонстрируют минимальную заинтересованность в учебной, познавательной и творческой деятельности, составляющей содержание программы. На итоговом тестировании показывают минимальное знание теоретического материала, практическое применение знаний воплощается в продукт, требующий руководящей помощи педагога.

Критерии оценки достижения планируемых результатов

Оценка достижения планируемых результатов освоения программы осуществляется по достаточному и минимальному уровню.

Оценочные материалы — пакет диагностических методик, позволяющих определить достижение учащимися планируемых результатов, представлен в приложениях программы.

4. Критерии оценки знаний, умений и навыков при освоении программы

Для того чтобы оценить усвоение программы, в течение года используются следующие методы диагностики: собеседование, наблюдение, выполнение отдельных творческих заданий, тестирование.

Применяется 3-х балльная система оценки знаний, умений и навыков обучающихся (выделяется три уровня: ниже среднего, средний, выше среднего).

Уровень освоения программы *ниже среднего* – ребёнок овладел менее чем 50% предусмотренных знаний, умений и навыков, испытывает серьёзные

затруднения при работе с учебным материалом; в состоянии выполнять лишь простейшие практические задания педагога.

Средний уровень освоения программы – объём усвоенных знаний, приобретённых умений и навыков составляет 50-70%; работает с учебным материалом с помощью педагога; в основном, выполняет задания на основе образца; удовлетворительно владеет теоретической информацией по темам курса.

Уровень освоения программы *выше среднего* – учащийся овладел на 70-100% предусмотренным программой учебным планом; работает с учебными материалами самостоятельно, не испытывает особых трудностей; свободно владеет теоретической информацией по курсу, применяет полученную информацию на практике.

Формы контроля качества образовательного процесса:

- собеседование,
- наблюдение,
- выполнение творческих заданий и проекта,
- тестирование.

5. Список использованных источников и литературы

1. Агитова, С. Ю. Защита детей от ситуаций, угрожающих их жизни, здоровью иразвитию / С. Ю. Агитова // Социальная педагогика. – 2015. – № 4. – С. 23–32.

2. Агрба, Л. М. Образовательный веб-квест "Безопасность в сети Интернет" / Л. М.Агрба // Информатика в школе. – 2015. – № 1. – С. 6–16.

3. Богданова, Д. А. Обучение Интернет-безопасности в начальных и младших классахсредней школы / Д. А. Богданова, Г. Р. Буркатовская // Народное образование. – 2015. – № 4. – С. 213–219.

4. Букина, Е. Ю. Формирование у младших школьников навыков безопасной работы всети Интернет / Е. Ю. Букина // Информатика в школе. – 2014. – № 5. – С. 40–49.

5. Рассказова, Е. И. Риски и угрозы в Интернет для детей и подростков / Е. И.

Рассказова, С. В. Чигарькова // Основыбезопасности жизнедеятельности. – 2014. – № 1. – С. 41–46.

6. Симонова, И. В. Понятийный аппарат знаний об информационной безопасности вшкольном курсе информатики / И. В. Симонова, М. И. Бочаров // Педагогическая информатика. – 2013. – № 4. – С. 42–50

Интернет – ресурсы

1. Дети России Онлайн http://detionline.com/

2. Информационный ресурс «Персональные данные дети» http://персональныеданные.дети

3. Информационный ресурс «Азбука цифрового мира» https://edu.yar.ru/azbuk

4. Международный квест по цифровой грамотности «Сетевичок» https://сетевичок.рф

5. Центр безопасного интернета в России https://www.saferunet.ru/children/

Диагностический инструментарий

Тест по безопасности в сети Интернет

1. Что является основным каналом распространения компьютерных вирусов?
    1) Веб-страницы;
    2) Электронная почта;
    3) Флеш-накопители (флешки).

2. Для предотвращения заражения компьютера вирусами следует:
    1) Не пользоваться Интернетом;
    2) Устанавливать и обновлять антивирусные средства;
    3) Не чихать и не кашлять рядом с компьютером,

3. Если вирус обнаружен, следует:
    1) Удалить его и предотвратить дальнейшее заражение;
    2) Установить, какую разновидность имеет вирус;
    3) Выяснить, как он попал на компьютер.

4. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
    1) Применение брандмауэра;
    2) Обновления операционной системы;
    3) Антивирусная программа.

5. Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?
    1) Уничтожение компьютерных вирусов;
    2) Создание и распространение компьютерных вирусов и вредоносных программ;
    3) Установка программного обеспечения для защиты компьютера.

Осторожно, Интернет!

1. Какую информацию нельзя разглашать в Интернете?
    1) Свои увлечения;
    2) Свой псевдоним;
    3) Домашний адрес.

2. Чем опасны социальные сети?
    1) Личная информация может быть использована кем угодно в разных целях;
    2) При просмотре неопознанных ссылок компьютер может быть взломан;
    3) Все вышеперечисленное верно.

3. Виртуальный собеседник предлагает встретиться, как следует поступить?
    1) Посоветоваться с родителями и ничего не предпринимать без их согласия;
    2) Пойти на встречу одному;
    3) Пригласить с собой друга.

4. Что в Интернете запрещено законом?
    1) Размещать информацию о себе;
    2) Размещать информацию других без их согласия;
    3) Копировать файлы для личного использования.

5. Действуют ли правила этикета в Интернете?
    1) Интернет - пространство свободное от правил;
    2) В особых случаях;
    3) Да, как и в реальной жизни.

Тест по безопасности в сети Интернет

1. Как могут распространяться компьютерные вирусы?
   1) Посредством электронной почты.
   2) При просмотре веб-страниц.
   3) Через клавиатуру.
   4) Их распространяют только преступники.

2. Зачем нужен брандмауэр?
   1) Он не дает незнакомцам проникать в компьютер и просматривать файлы.
   2) Он защищает компьютер от вирусов.
   3) Он обеспечивает защиту секретных документов.
   4) Он защищает компьютер от пожара.

3. Всегда ли можно быть уверенным в том, что электронное письмо было получено от указанного отправителя?
   1) Да.
   2) Да, если вы знаете отправителя.
   3) Нет, поскольку данные отправителя можно легко подделать.
   4) Может быть.

4. На компьютере отображается непонятное сообщение. Какое действие предпринять?
   1) Продолжить, будто ничего не произошло.
   2) Нажать кнопку «ОК» или «ДА»
   3) Обратится за советом к учителю, родителю или опекуну.
   4) Больше никогда не пользоваться Интернетом

5. Что нужно сделать при получении подозрительного сообщения электронной почтой?
   1) Удалить его, не открывая.
   2) Открыть его и выяснить, содержится ли в нем какая-нибудь важная информация.
   3) Открыть вложение, если такое имеется в сообщении.
   4) Отправить его родителям

6. В ящик входящей почты пришло «письмо счастья». В письме говорится, чтобы его переслали пяти друзьям. Какое действие предпринять?
   1) Переслать его пяти друзьям.
   2) Переслать его не пяти друзьям, а десяти друзьям.
   3) Не пересылать никакие «письма счастья»
   4) Ответить отправителю, что вы больше не хотите получать от него/нее письма.

7. В каких случаях можно, не опасаясь последствий, сообщать в Интернете свой номер телефона или домашний адрес?
   1) Во всех случаях.
   2) Когда кто-то просит об этом.
   3) Когда собеседник в чате просит об этом.
   4) Такую информацию следует с осторожностью сообщать людям, которым вы доверяете.

8. Вы случайно прочитали пароль, который ваш друг записал на листочке бумаг. Как вы должны поступить?
   1) Запомнить его.
   2) Постараться забыть пароль.
   3) Сообщить другу, что вы прочитали пароль, и посоветовать сменить пароль и никогда больше не записывать на листе бумаги.
   4) Сообщить пароль родителям.

9. Что такое сетевой этикет?
   1) Правила поведения за столом.
   2) Правила дорожного движения.
   3) Правила поведения в Интернете.
   4) Закон, касающийся Интернета.

10. Что запрещено в интернете?
   1) Запугивание других пользователей.
   2) Поиск информации.
   3) Игры.
   4) Общение с друзьями.

государственное бюджетное общеобразовательное учреждение Самарской области «Школа-интернат для обучающихся с ограниченными возможностями здоровья с. Обшаровка Приволжского района Самарской области»

Адрес: 445550, Самарская область, Приволжский район, с. Обшаровка, ул. Советская, 98, Телефон (факс): (84647) 93236, mail: gscou_prv@63edu.ru

Календарно-тематическое планирование по курсу «Цифровая гигиена» предметная область «Внеурочная деятельность» 6-9 классы

Составитель: Рафейчик Ольга Александровна

учитель высшей квалификационной категории

Обшаровка, 2025-2026 учебный год

№ п/п	Тема.	Количество часов			Дата
		6 класс	7 класс	8-9 класс	
	«Безопасность общения» - 14 часов				
1.	Общение в социальных сетях и мессенджерах	1	1	1	
2.	С кем безопасно общаться в интернете	1	1	1	
3.	Пароли для аккаунтов социальных сетей	1	1	1	
4.	Безопасный вход в аккаунты	1	1	1	
5.	Настройки конфиденциальности в социальных сетях	1	1	1	
6.	Публикация информации в социальных сетях	1	1	1	
7.	Кибербуллинг	1	1	1	
8.	Публичные аккаунты	1	1	1	
9.	Фишинг	2	2	2	
10.	Выполнение и защита индивидуальных и групповых проектов	4	4	4	
	«Безопасность устройств» - 9 часов				
1.	Что такое вредоносный код?	1	1	1	
2.	Распространение вредоносного кода	1	1	1	
3.	Методы защиты от вредоносных программ	2	2	2	
4.	Распространение вредоносного кода для мобильных устройств	1	1	1	
5.	Выполнение и защита индивидуальных и групповых проектов	4	4	4	
	«Безопасность информации» - 11 часов				
1.	Социальная инженерия: распознать и избежать	1	1	1	
2.	Ложная информация в Интернете	1	1	1	
3.	Безопасность при использовании платежных карт в Интернете	1	1	1	
4.	Беспроводная технология связи	1	1	1	
5.	Резервное копирование данных	1	1	1	
6.	Основы государственной политики в области формирования культуры информационной безопасности	2	2	2	
7.	Выполнение и защита индивидуальных и групповых проектов	4	4	4	
	Итого:	34	34	34	
		102 часа			