Ядыкина
Ульяна
Михайловна
воспитатель ГКОУ
школы-интерната №2
г. Армавира

4. Результативность деятельности педагогического работника в профессиональном сообществе

4.1 Результаты участия педагогического работника в разработке программно – методического сопровождения образовательного процесса

4. Результативность деятельности педагогического работника в профессиональном сообществе

4.1 Результаты участия педагогического работника в разработке программно – методического сопровождения образовательного процесса

РЕЦЕНЗИЯ

на программу факультатива

«Информационная безопасность»

воспитателя ГКОУ школы-интерната №2 города Армавира

Ядыкиной Ульяны Михайловны

Безопасность в сети Интернет, в свете быстрого развития информационных технологий, резко повышает потребность в воспитании у обучающихся культуры информационной безопасности в целях предотвращения негативных последствий массового использования Интернета детьми и их защиты от агрессивной и противоправной информации.Особой потребностью в воспитании культуры информационной безопасности нуждаются обучающиеся с нарушениями слуха, так как полное или частичное отсутствие слуха не только нарушает социальную адаптацию человека, но влияет на его психическое развитие.

Представленная на рецензию программа по курсу факультатива «Информационная безопасность» построена в соответствии с последними требованиями федерального государственного образовательного стандарта школьного образования.

Рецензируемая программа основана на создании условий для профилактики негативных воздействий информации на психологическое состояние личности обучающихся с нарушениями слуха, посредством формирования компетенций, способствующих обеспечению информационно-психологической безопасности школьников.

Актуальность программы внеурочной деятельности «Информационная безопасность» обусловлена также отсутствием на сегодняшний день комплексных образовательных продуктов, направленных на формирование навыков безопасного использования Интернета, профилактику интернет-зависимости, предназначенных для реализации в рамках учебно-воспитательной работы образовательной организации.Помимо профилактики информационных угроз и противоправных действий через ресурсы в сети Интернет и мобильные сети, программа предполагает использование коммуникации для привлечения обучающихся с нарушениями слуха к информационно-учебной и познавательно-творческой активности по использованию позитивных интернет-ресурсов: учебных, культурных, научно-популярных, интеллектуальных, читательских, медийных, познавательных и специализированных социальных сообществ и сервисов для детских объединений и творческих мероприятий для детей и молодежи.

Программа построена на основании принципов групповой и индивидуальной работы с учётом возрастных особенностей и особых образовательных потребностей участников. В программе обоснована ее актуальность, определена цель и конкретизированы задачи программы.

Программа факультатива «Информационная безопасность» согласуется с целями и задачами основной общеобразовательной программы основного общего образования.

Срок реализации программы – 6 лет. По окончании курса по данной программе у детей имеется необходимый багаж знаний, умений и навыков, которые помогут им успешно социализироваться в мир слышащих людей, которые они будут использовать на практике.

Автором программы определены ожидаемые результаты и отмечена важность ориентации на личность обучающихся с нарушениями слуха, развитие их индивидуальных способностей, что усиливает социальную защищенность выпускников.

Программа соответствует требованиям Министерства образования РФ,специфике данного учреждения. Целесообразно рекомендовать к использованию в специальных коррекционных образовательных учреждениях для детей с нарушениями слуха.

Рецензент:
к.п.н., зав. кафедры
ССПиП ФГБОУ ВО «АГПУ» А.М. Дохоян

МИНИСТЕРСТВО ОБРАЗОВАНИЯ НАУКИ И МОЛОДЁЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ СПЕЦИАЛЬНАЯ (КОРРЕКЦИОННАЯ) ШКОЛА-ИНТЕРНАТ № Г. АРМАВИРА

Утверждено
решением педсовета
от «30» августа 2023 года
протокол №1
Председатель педсовета
М.Н. Зиновская

РАБОЧАЯ ПРОГРАММА ФАКУЛЬТАТИВА

ФГОС 1.2

По курсу	информационная безопасность
Уровень образования (класс):	основное общее, 5-10 классы
Количество часов	204 часа
Составитель	Ядыкина У.М.

Программа разработана на основе адаптированной основной общеобразовательной программы основного общего образования для глухих обучающихся ГКОУ школы-интерната №2 г. Армавира, составленной в соответствии с ФГОС ООО (приказ Министерства просвещения РФ от 31.05.2021г. № 287) и ФАОП ООО для обучающих с ОВЗ(приказ Министерства просвещения РФ от 24 ноября 2022 г. №1025)иутвержденной решением педагогического совета, протокол №1 от 30.08.2023года

1. Пояснительная записка.

Рабочая программа курса «Информационная безопасность» составлена на основе:

– Федерального государственного образовательного стандарта основного общего образования (утвержденного приказом Министерства просвещения Российской Федерации от 31 мая 2021 года № 287);

- Адаптированной основной общеобразовательной программы основного общего образования для глухих обучающихся ГКОУ школы-интерната №2 г. Армавира, составленной в соответствии с ФГОС ООО (приказ Министерства просвещения РФ от 31.05.2021г. № 287) и ФАОП ООО для обучающих с ОВЗ (приказ Министерства просвещения РФ от 24 ноября 2022 г. №1025)

Рабочая программа для обучающихся с нарушениями слуха представляет собой программу, адаптированную для воспитания и социализации глухих обучающихся с учетом их особых образовательных потребностей, в том числе обеспечивающая коррекцию нарушений развития.

Рабочая программа факультатива для глухих обучающихся учитывает следующие принципы:

- принцип индивидуализации обучения: разработки программ и учебных планов для обучающихся с нарушениями слуха с учетом мнения родителей (законных представителей) обучающегося;
- принцип учета индивидуальных возрастных, психологических и физиологических особенностей глухих обучающихся при построении образовательного процесса и определении образовательно-воспитательных целей и путей их достижения;
- принцип интеграции обучения и воспитания: ФАОП СОО предусматривает связь урочной и внеурочной деятельности, предполагающий направленность учебного процесса на достижение личностных результатов освоения образовательной программы;
- принцип здоровьесбережения: при организации внеурочной деятельности не допускается использование технологий, которые могут нанести вред физическому и

- принцип здоровьесбережения: при организации внеурочной деятельности не допускается использование технологий, которые могут нанести вред физическому и (или) психическому здоровью обучающихся, приоритет использования здоровьесберегающих педагогических технологий.

Рабочая программа для глухих обучающихся учитывает возрастные и психологические особенности обучающихся. Программа реализуется в рамках социального направления развития личности плана внеурочной деятельности.

Безопасность в сети Интернет в свете быстрого развития информационных технологий резко повышает потребность в воспитании у обучающихся культуры информационной безопасности в целях предотвращения негативных последствий массового использования Интернета детьми и их защиты от агрессивной и противоправной информации.

Особой потребностью в воспитании культуры информационной безопасности нуждаются глухие обучающиеся, так как полное отсутствие слуха не только нарушает социальную адаптацию человека, но влияет на его психическое развитие.

Программа устанавливает планируемые результаты освоения курса информационной безопасности основного общего образования для 5–10классов.

Главная **цель** курса – обеспечить социальные аспекты информационной безопасности в воспитании глухих обучающихся в условиях цифрового мира, включение цифровой гигиены в контекст воспитания детей на регулярной основе, формирование у глухого выпускника школы правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию детей в информационном обществе, формирование личностных и метапредметных результатов обучения и воспитания детей.

Задачи:

- формировать понимание сущности и воспитывать необходимость принятия глухими обучающимися таких ценностей, как ценность человеческой жизни, свободы, равноправия и достоинства людей, здоровья, опыта гуманных, уважительных отношений с окружающими;
- создавать педагогические условия для формирования правовой и информационной культуры глухих обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствия деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;
- формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;
- мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;
- обеспечить планируемые результаты по освоению обучающимися целевых установок, приобретению знаний, умений и навыков, определяемых личностными, семейными, общественными, государственными потребностями и возможностями обучающегося, индивидуальными особенностями его развития и состояния здоровья;
- обеспечить преемственность основного общего общего образования;
- научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны – России в условиях развития цифрового мира, ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

1. Общая характеристика курса.

Курс факультатива «Информационная безопасность» относится к направлению социального воспитания.

Программа имеет высокую актуальность и отражает важные вопросы безопасной работы с новыми формами коммуникаций и услуг цифрового мира: потребность в защите персональной информации, угрозы, распространяемые глобальными средствами коммуникаций Интернета и мобильной связи, использующими рассылки сообщений, электронную почту, информационно-коммуникативные ресурсы взаимодействия в сети Интернет через массово доступные услуги электронной коммерции, социальные сервисы, сетевые объединения и сообщества, ресурсы для досуга (компьютерные игры, видео и цифровое телевидение, цифровые средства массовой информации и новостные сервисы), а также повсеместное встраивание дистанционных ресурсов и технологий в учебную деятельность, использующую поиск познавательной и учебной информации, общение в социальных сетях, получение и передачу файлов, размещение личной информации в коллективных сервисах. Помимо профилактики информационных угроз и противоправных действий через ресурсы в сети Интернет и мобильные сети, использовать коммуникации для привлечения глухих обучающихся к информационно-учебной и познавательно-творческой активности по использованию позитивных интернет-ресурсов: учебных, культурных, научно-популярных, интеллектуальных, читательских, медийных, познавательных и специализированных социальных сообществ и сервисов для детских объединений и творческих мероприятий для детей и молодежи.

2. Описание курса в учебном плане.

Согласно учебному плану ГКОУ школы-интерната № 2 г. Армавира курс факультатива «Информационная безопасность» входит в часть, формируемую участниками образовательных отношений. Общее число часов за 6 лет основной школы (5-10 класс) составляет 204 часа: 34 часа в год, 1 час в неделю.

3. Ценностные ориентиры содержания курса.

Изучение курса вносит значительный вклад в достижение главных целей основного общего образования, способствуя:

- *формированию целостного мировоззрения*, соответствующего современному уровню развития науки и общественной практики за счет развития представлений об информации как важнейшем стратегическом ресурсе развития личности, государства, общества; понимания роли информационных процессов в современном мире;
- *совершенствованию общеучебных и общекультурных навыков работы с информацией* в процессе систематизации и обобщения имеющихся и получения новых знаний, умений и способов деятельности в области информатики и ОБЖ; развитию навыков самостоятельной учебной деятельности глухих школьников (учебного проектирования, моделирования, исследовательской деятельности и т.д.);
- *воспитанию ответственного и избирательного отношения к информации* с учетом правовых и этических аспектов ее распространения, воспитанию стремления к продолжению образования и созидательной деятельности с применением средств ИКТ.

4. Личностные, метапредметные и предметные результаты освоения курса.

В соответствии с Федеральным государственным образовательным стандартом основного общего образования обучающихся с ОВЗ необходимо сформировать у глухих обучающихся, учитывая их особые образовательные потребности и индивидуальные особенности, такие ***личностные результаты***, которые позволят им грамотно ориентироваться в информационном мире с учетом имеющихся в нем угроз:

- принимать ценности человеческой жизни, семьи, гражданского общества, многонационального российского народа, человечества;
- быть социально адаптированными, уважающими закон и правопорядок, соизмеряющими свои поступки с нравственными ценностями, осознающими свои обязанности перед семьей, обществом, Отечеством;
- уважать других людей, достигать взаимопонимания, сотрудничать для достижения общих результатов;
- осознанно выполнять правила здорового образа жизни, безопасного для человека и окружающей его среды.

В результате освоения Программы курса информационной безопасности акцентируется внимание на ***метапредметных результатах*** освоения программы глухими обучающимися:

- *коммуникативных:*
  - освоение социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах, включая взрослые и социальные сообщества; участие в школьном самоуправлении и общественной жизни в пределах возрастных компетенций с учетом особенностей здоровья;
  - готовность конструктивно разрешать конфликты посредством учета интересов сторон и сотрудничества;
- *познавательных:*
  - активное использование средств информационно-коммуникационных технологий (ИКТ) для решения познавательных и организационных задач, с соблюдением требований техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;
- *регулятивные:*
  - готовность и способность к самостоятельной информационно-познавательной деятельности, включая умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;
  - умение излагать свое мнение, аргументировать свою точку зрения и оценивать результаты своей деятельности.

Планируется достижение ***предметных результатов***:

- формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права;
- освоение приемов работы с социально значимой информацией, ее осмысление; развитие способностей обучающихся делать необходимые выводы и давать обоснованные оценки социальным событиям и процессам.

В результате освоения программы с учетом возрастных и индивидуальных особенностей глухой выпускник освоит жизненно важные практические компетенции.

Выпускник научится понимать:

- источники информационных угроз, вредоносные программы и нежелательные рассылки, поступающие на мобильный телефон, планшет, компьютер;
- роль близких людей, семьи, школы для устранения проблем и угроз в сети Интернет и мобильной телефонной связи, телефоны экстренных служб;
- виды информационных угроз, правила поведения для защиты от угроз;
- проблемные ситуации и опасности в сетевом взаимодействии и правила поведения в проблемных ситуациях, ситуациях профилактики и предотвращения опасности;
- этикет сетевого взаимодействия;
- простейшие правила защиты персональных данных;
- назначение различных позитивных ресурсов в сети Интернет для образования и развития творчества.

Выпускник научится применять на практике:

- простейшие правила цифровой гигиены для использования средств защиты персональных данных (формировать и использовать пароль, регистрироваться на сайтах без распространения личных данных);
- начальные компетенции компьютерной грамотности по защите персональных устройств от вредоносных программ при работе с информацией в сети Интернет, критическое и избирательное отношение к источникам информации;
- информационно-коммуникативные компетенции по соблюдению этических и правовых норм взаимодействия в социальной сети или в мессенджере, умение правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.), отключаться от нежелательных

контактов, действовать согласно правовым нормам в сфере информационной безопасности (защиты информации).

Выпускник освоит нормы культуры информационной безопасности в системе универсальных учебных действий для самостоятельного использования в учебно-познавательной и досуговой деятельности позитивного Интернета и средств электронного обучения с соблюдением правил информационной безопасности.

5. Содержание учебного курса.

Особенностью курса является постепенное усложнение учебного материала для разных возрастных групп обучающихся с нарушениями слуха, с учётом их особенностей. Курс представлен шестью блоками дляобучающихся5, 6, 7, 8, 9 и 10классов. Каждый блок имеет несколько разделов.

5 класс

Раздел «Правила безопасной работы в сети Интернет с мобильным телефоном» - 16 часов.

История создания мобильного телефона. Мобильный телефон и его функции. Сотовая связь. Мобильные сети связи. СМС от неизвестных лиц. Ложные сообщения. Угрозы в СМС. СМС с предложениями. Защита от входа в твой телефон. Подключение телефона к «Wi-Fi» сети. Вызов экстренных служб. Телефонное хулиганство. Правила хороших манер. Мобильный телефон в школе. Угрозы в мобильных сетях связи. Мобильные мошенники.

Раздел «Правила безопасной работы в сети Интернет с планшетом или на компьютере» - 18 часов.

Как появился компьютер. Устройство компьютера. Компьютеру тоже нужна забота (как ухаживать за ПК). Компьютер и здоровье школьника. Мой планшет или компьютер: защита входа. Персональные данные. Моя почта, логин и пароль. Спам. Почта от неизвестных лиц. Вирусы. Безопасный интернет. Личные данные. Регистрация на сайтах. Как искать полезную информацию. Вредные/полезные игры. Игровая зависимость.

6 класс.

Раздел «Правила безопасной работы в социальной сети» - 8 часов.

Что такое Аватар и как его выбрать. «Друг» в сети, кто за ним прячется. Ложные сообщения. Что говорить о себе незнакомцам. Спроси у взрослых. Этикет в общении. Защити себя от недоброжелателей. Уговоры и предложения. Отключение от нежелательных контактов.

Раздел«Путешествуем в сети Интернет» - 26 часов.

Поиск информации в Интернете. Сайты для детей. Сайты о безопасном поведении. Сайты для учебы. Сайты с электронными книгами. Сайты с коллекциями для детей. Популярные информационно-поисковые системы.

7 класс.

Раздел «Что такое информационное общество?» - 29 часов.

Что такое информационное общество. Что нужно знать? Пространство Интернета на планете Земля. История создания сети Интернет. Что такое Всемирная паутина. Путешествие по сети Интернет: сайты и электронные сервисы. Как стать пользователем Интернета. Опасности для пользователей Интернета. Что такое кибератака. Кибербуллинг и фишинг. Что такое информационная безопасность. Законы о защите личных данных в Интернете. Сетевой этикет. Защита персональных данных. Детская безопасность в интернете. Контент. Закон о защите детей.

Раздел «Электронные музеи» - 5 часов.

Русский музей в Санкт-Петербурге. Третьяковская галерея в Москве. Музей изобразительных искусств имени А. С. Пушкина в Москве. Эрмитаж. Политехнический музей в Москве.

8 класс.

Раздел «Что нужно уметь? Правила для пользователей сети Интернет» - 26 часов.

Правила работы с СМС в аккаунте. Приватность аккаунтов. Правила работы с электронной почтой. Сообщения со взломанных аккаунтов. Правила работы в социальной сети ВКонтакте. Компьютерные видеоигры. Правила работы в социальных сетях. Правила защиты от вирусов, спама, рекламы и рассылок. Мошенничество в интернете. Правила защиты от негативных сообщений. Правила общения в социальной сети. Система помощи

на страницах популярных соцсетей. Как вести себя в социальных сетях? Правила работы с поисковыми системами и анализ информации. Ложная информация. Правила ответственности за распространение ложной и негативной информации. Правила защиты от нежелательных сообщений и контактов. Правила вызова экстренной помощи. Правила защиты устройств от внешнего вторжения.

Раздел «Путешествия по полезным ресурсам сети Интернет» - 8 часов.

Полезные ресурсы в сети Интернет. Российская государственная детская библиотека. Национальная электронная детская библиотека. Средства работы в Интернете для людей с особыми потребностями.

9 класс.

Раздел «Киберпространство» - 29 часов.

Киберпространство. Определение и структура киберпространства. История возникновения киберпространства. Этап современных информационных технологий. Появление и развитие Интернет. Базовые понятия в киберпространстве. Браузеры. Язык киберпространства. Визуальное восприятие интернет-ресурса. Интернет, статистика и тренды. Виртуальная реальность. Большой скачок. Кибермиры. Киберфизическая система. Киберобщество. Киберденьги. Кибермошенничество.

Раздел «Онлайн-курс Академии Яндекс «Безопасность в Интернете» - 5 часов.

Защита от вредоносных программ. Безопасность аккаунтов. Безопасные онлайн-платежи.

10 класс.

Раздел «Киберкультура» - 19 часов.

Киберкультура. Путешествие в закулисный мир Большого театра. Московский планетарий. От книги к гипертексту. Киберкнига. Киберискусство. Социальная инженерия. Классификация угроз социальной инженерии. Меры безопасности при использовании банковских карт.

Раздел «Киберугрозы» - 4 часа.

Кибервойны. Киберпреступность и информационная преступность. Запрещенные и нежелательные сайты. Обзор антивирусного ПО.

Раздел «Профориентация» - 11 часов.

Рынок труда. Среднее специальное учебное заведение (ССУЗ).Учебные заведения среднего профессионального образования г.Армавира, Краснодарского края, России. Моя профессия.

6. Тематическое планирование курса.

№	Разделы	Количество часов
5 класс		
1.	Правила безопасной работы в сети Интернет с мобильным телефоном.	16
2.	Правила безопасной работы в сети Интернет с планшетом или на компьютере.	18
6 класс		
3.	Правила безопасной работы в социальной сети.	8
4.	Путешествуем в сети Интернет.	26
7 класс		
5.	Что такое информационное общество?	29
6.	Электронные музеи.	5
8 класс		
7.	Что нужно уметь? Правила для пользователей сети Интернет.	26
8.	Путешествия по полезным ресурсам в сети Интернет.	8
9 класс		
9.	Киберпространство.	29
10.	Онлайн курс Академии Яндекс «Безопасность в Интернете».	5

10 класс		
1.	Киберкультура.	19
2.	Киберугрозы.	4
3.	Профориентация.	11

№	Тема	Кол-во часов	Характеристика основных видов деятельности учащихся
5 класс			
Раздел «Правила безопасной работы в сети Интернет с мобильным телефоном» (16 часов)			
1.	История создания мобильного телефона.	1	Знакомятся с историей создания сотового телефона. Учатся давать определение понятиям мобильный телефон, сотовая связь.
2.	Мобильный телефон и его функции.	1	Рисуют свой мобильный телефон. Учатся безопасно использовать средства коммуникации.
3.	Сотовая связь. Мобильные сети связи.	1	Отвечают на вопрос: Какие услуги предоставляют операторы сотовой связи? Знакомятся с различными операторами сотовой связи.
4.	СМС от неизвестных лиц.	1	Учатся знать и понимать источники угроз, поступающих на мобильный телефон. Проходят тест.
5.	Ложные сообщения.	1	Учатся распознавать ложные сообщения, проблемные ситуации в сетевом взаимодействии.
6.	Угрозы в СМС.	1	Знакомятся с видами угроз в СМС. Узнают правила поведения для защиты от угроз. Учатся правильно вести себя в проблемной ситуации.
7.	СМС с предложениями.	1	Учатся дифференцировать СМС с предложениями, распознавать рекламные предложения, проблемные ситуации в сетевом взаимодействии
8.	Защита от входа в твой телефон.	1	Учатся формировать и использовать пароль. Учатся ставить пароль на телефон,
9.	Подключение телефона к «Wi-Fi» сети.	1	Изучают возможности сети «Wi-Fi». Учатся безопасно использовать средства коммуникации.
10.	Вызов экстренных служб.	1	Учатся вызывать экстренные службы с мобильного телефона. Учатся использовать средства связи в решении когнитивных и коммуникативных задач.
11.	Телефонное хулиганство.	1	Знакомятся с понятием «телефонное хулиганство». Учатся правильно вести себя в проблемной ситуации.
12.	Правила хороших манер.	1	Учатся соблюдать правила хороших манер в сети Интернет. Осваивают социальные нормы, правила поведения, роли и формы социальной жизни в группах и сообществах.
13.	Мобильный телефон в школе.	1	Изучают правила пользования мобильным телефоном в школе. Учатся осознанно выполнять правила поведения в школе-интернате.
14.	Угрозы в мобильных сетях связи.	1	Знакомятся с видами угроз. Узнают правила поведения для защиты от угроз.
15.	Мобильные мошенники.	1	Отвечают на вопрос: кто такие мобильные мошенники и чем они опасны? Учатся правильно вести себя в проблемной ситуации.
16.	Итоговое занятие.	1	Составляют памятку правил

			пользования мобильным телефоном.
Раздел «Правила безопасной работы в сети Интернет с планшетом или на компью-тере»(18 часов)			
1.	Как появился компьютер.	1	Знакомятся с историей создания компьютера. Учатся давать определение понятию персональный компьютер.
2.	Устройство компьютера.	1	Рисуют свой компьютер. Знакомятся с устройством компьютера.
3.	Компьютеру тоже нужна забота (как ухаживать за ПК).	1	Отвечают на вопросы. Формируют навыки и умения безопасного и целесообразного поведения при работе с компьютером.
4.	Компьютер и здоровье школьника.	1	Изучают проблему влияния компьютера на здоровье школьника. Учатся осознанно выполнять правила здорового и образа жизни, безопасного для человека. Учатся понимать и принимать ценности человеческой жизни.
5.	Мой планшет или компьютер: защита входа.	1	Учатся формировать и использовать пароль, ставить пароль на компьютер/планшет.
6.	Персональные данные.	1	Знакомятся с понятием «персональные данные». Учатся регистрироваться на сайтах без распространения личных данных.
7.	Моя почта, логин и пароль.	2	Знакомятся с понятиями: «логин», «пароль». Создают свой почтовый ящик.
8.	Спам.	1	Знакомятся с понятием спам и его видами. Учатся использовать позитивный Интернет.
9.	Почта от неизвестных лиц.	1	Учатся безопасно пользоваться электронной почтой. Учатся правильно вести себя в проблемной ситуации.
10.	Вирусы.	1	Знакомятся с вирусами в Интернете и методам борьбы с ними. Узнают правила поведения для защиты от вирусов.
11.	Безопасный интернет.	1	Смотрят видеоурок «СПАС Экстрим. *Безопасный интернет*».
12.	Личные данные.	1	Знакомятся с правилами введения личных данных при регистрации на сайте в сети Интернет. Учатся регистрироваться на сайтах без распространения личных данных.
13.	Регистрация на сайтах.	1	Учатся регистрироваться на популярных и полезных сайтах (одноклассники, ВКонтакте, для учёбы и т.д.)
14.	Как искать полезную информацию.	1	Знакомятся с полезными сайтами для детей. Учатся использовать позитивный Интернет.
15.	Вредные/полезные игры.	1	Обсуждают виды интернет-игр. Учатся безопасно использовать ресурсы интернета.
16.	Игровая зависимость.	1	Знакомятся с последствиями игровой зависимости. Учатся основам самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности
17.	Контрольное занятие.	1	Составляют личную памятку

			безопасности в сети Интернет.
6 класс			
№	**Тема**	**Кол-во часов**	**Характеристика основных видов деятельности учащихся**
Раздел «Правила безопасной работы в социальной сети» (8 часов)			
1.	Что такое Аватар и как его выбрать.	1	Знакомятся с понятием «аватар», правилами размещения фотографии в сети Интернет.
2.	«Друг» в сети, кто за ним прячется.	1	Знакомятся с видами и формами мошенничества в социальной сети.
3.	Ложные сообщения.	1	Знакомятся с видами и формами мошенничества в сети интернет. Учатся распознавать ложные сообщения, проблемные ситуации в сетевом взаимодействии.
4.	Что говорить о себе незнакомцам. Спроси у взрослых.	1	Обсуждают правила разглашения личной информации.
5.	Этикет в общении: – нельзя обижать; – если тебя обижают.	1	Знакомятся с правилами этикета общения в сети Интернет. Учатся уважать других людей, уметь вести конструктивный диалог, достигать взаимопонимания.
6.	Защити себя от не доброжелателей: – если тебе угрожают; – агрессия и грубость.	1	Обсуждают способы защиты от недоброжелателей в сети Интернет. Учатся распознавать ложные сообщения, проблемные ситуации в сетевом взаимодействии.
7.	Уговоры и предложения. Отключение от нежелательных контактов.	1	Обсуждают виды нежелательных предложений через сети Интернет и способы их отключения. Учатся распознавать ложные сообщения, проблемные ситуации в сетевом взаимодействии
8.	Контрольное занятие.	1	Изучают материал на Портале детской безопасности Министерства чрезвычайных ситуаций нс страничке Темы «Интернет-безопасность». Участвуют в викторине.
Раздел «Путешествуем в сети Интернет» (26 часов)			
1.	Поиск информации в Интернете.	1	Учатся находить полезную информацию в сети Интернет.
2.	Сайты для детей.	2	Знакомятся с материалами сайта Детская игровая комната и используют их для разнообразия своего досуга. Знакомятся с материалами сайта Страна Мастеров.
3.	Сайты о безопасном поведении.	4	Изучают материал на Портале детской безопасности Министерства чрезвычайных ситуаций нс страничке Темы. Используют материалы сайта для самостоятельной работы.
4.	Сайты для учебы.	8	Знакомятся с сайтами для учёбы и используют их для онлайн-обучения: – Детская энциклопедия Потому.ру; – Детская онлайн-энциклопедия «Хочу всё знать»; – Электронное учебное пособие «Учимся беречь энергию» – размещено в открытом доступе; – СайтLingualeo. «Покори язык»; – Учи.ру;

			– Российская электронная школа; – Московский планетарий; – Московский зоопарк; – Культура России.
5.	Сайты с электронными книгами.	2	Знакомятся с сайтом Национальная электронная детская библиотека. Регистрируются в библиотеке, пользуются ресурсами. Выбирают и скачивают книгу для внеклассного чтения.
6.	Сайты с коллекциями для детей.	4	Знакомятся с сайтами и их разделами: – Лукошко – Журнал «Мурзилка» Знакомятся с уроками безопасности для детей на сайте Теремок. На сайте Российской Государственной Детской Библиотеки на Главной странице выбирают Отделы в Отделе творческого развития читателей участвуют в мастер-классе по оригами «Бумажный зоопарк».Выбирают фигуру оригами и складывают ее по алгоритму Уроки оригами.
7.	Популярные информационно-поисковые системы.	4	Входят на сайт популярной информационно-поисковой системы Яндекс. Вводят в графу для поиска ключевые слова: – российская детская библиотека; – союзмультфильм; – союзфильм. Переходят на нужный сайт и добавляют его в систему закладок, используя
			сочетания клавиш Ctrl+D.
8.	Контрольное занятие.	1	Находят при помощи информационно-поисковой системы Яндекс сайты олимпиад или конкурсов по любимому им предмету. Выбирают интересный для них конкурс. Переходят на нужные сайты и добавляют их в систему закладок, используя сочетания клавиш Ctrl+D.

7 класс

№	Тема	Кол-во часов	Характеристика основных видов деятельности учащихся
Раздел «Что такое информационное общество?» (29 часов)			
1.	Введение. Что такое информационное общество.	1	Обсуждают в группе, какую опасность здоровью может нанести неразумное увлечением общением в сети Интернет-лайкомания.
2.	Что нужно знать? Пространство Интернета на планете Земля	2	Обсуждают в группе, какие угрозы таит в себе Интернет. – Угрозы Интернета для детей. – Мировой опыт защиты детей в Интернете.
3.	История создания сети Интернет.	2	Знакомятся с историей создания сети Интернет. Придумывают кроссворд на базе слова «Интернет».
4.	Что такое Всемирная паутина.	2	Знакомятся с сайтом телеканала «Карусель» просматривают разделы сайта. Знакомятся с понятием«веб-браузер»
5.	Путешествие по сети Интернет: сайты и электронные сервисы.	2	Выполняют поиск сайта телеканала «Карусель» с помощью поисковой системы Яндекс. Выбирают нужную ссылку и переходят на этот сайт. Отвечают на

			вопрос: что такое поисковые системы и для чего они предназначены? Знакомятся с сайтом «Культура.РФ». Обсуждают в группе, какие разделы они находят наиболее интересными для себя, что понравилось больше всего.
6.	Как стать пользователем Интернета.	1	Знакомятся со способами выхода в Интернет» - Отвечают на вопрос: какие различные способы выхода в Интернет вы можете применять?
7.	Опасности для пользователей Интернета.	2	На сайте Большой Российской Энциклопедии: переходят в раздел «Россия» и знакомятся с рубриками раздела. Отвечают на вопрос: что такое информация? Обсуждают виды опасностей для пользователей сети Интернет.
8.	Что такое кибератака.	2	Знакомятся с понятием «кибератака». Отвечают на вопросы: что такое компьютерный вирус? Чем он опасен для компьютера? Знакомятся с понятиями: кибербуллинг и фишинг.
9.	Что такое информационная безопасность.	1	Составляют личную памятку безопасности при работе в Интернете.
10.	Законы о защите личных данных в Интернете.	2	Знакомятся с понятием «Защита персональных данных детей» на портале «Лига безопасного Интернета». Проходят электронный тест «Что ты знаешь о персональных данных» на сайте «Персональныеданные.
			Дети». Обсуждают в группе, что такое конфиденциальность и зачем ее соблюдать в Интернете. Какие угрозы подстерегают в сетевых играх? Обсуждают в группе, что такое конфиденциальность в интернете и правила общение в игре.
11.	Сетевой этикет.	2	Знакомятся с правилами поведения в коллективе/Сетевой этикет». Отвечают на вопрос: какие правила поведения в коллективе нужно использовать в сообщениях на мобильном телефоне или по электронной почте? Обсуждают в группе, какие правила нужно соблюдать при общении в Интернете, чтобы не навредить себе.
12.	Защита персональных данных. Детская безопасность в интернете.	1	Обсуждают правила пользования компьютером. Учатся правильно вести себя в проблемной ситуации.
13.	Детская безопасность в интернете.	1	Знакомятся с Законом «О защите детей от информации, причиняющей вред их здоровью и развитию». Обсуждают опасные контенты.
14.	Коллекции сайтов для детей.	7	Обсуждаю в группе, что такое «позитивный контент». Знакомятся с разделами интернет-браузера «Гогуль: Играй, Гуляй, Общайся, Учись». Создают своими руками из бумаги собственного Гогуля, следуя инструкции на

			страничке сайта Федеральной программы безопасного детского интернета «Гогуль» Путешествуют по ресурсам сайта «ВебЛандия». Обсуждают в группе, какие из них помогут в развитии творчества.
15.	Контрольное занятие.	1	Участвуют в викторине «Безопасность в интернете»
Раздел «Электронные музеи» (5 часов)			
1.	Русский музей в Санкт-Петербурге.	1	Знакомятся с виртуальными экскурсиями по Русскому музею.
2.	Третьяковская галерея в Москве.	1	Знакомятся с залами Музея. Учатся использовать позитивный Интернет.
3.	Музей изобразительных искусств имени А. С. Пушкина в Москве.	1	Знакомятся с музеем. Выбирают тематику и посещают электронную экспозицию Музея изобразительных искусств имени А. С. Пушкина.
4.	Эрмитаж.	1	Выбирают тур виртуального путешествия по Эрмитажу.
5.	Политехнический музей в Москве.	1	Знакомятся с музеем. Выбирают тур на сайте Политехнического музея и знакомятся с его экспозицией.

8 класс

№	Тема	Кол-во часов	Характеристика основных видов деятельности учащихся
Раздел «Что нужно уметь? Правила для пользователей сети Интернет» (26 часов)			
1.	Правила работы с СМС в аккаунте.	1	Обсуждают в группе виды возможного вымогательства денег через сообщения.
2.	Приватность аккаунтов.	1	Настраивают конфиденциальность на своей страничке в сети Интернет.
3.	Правила работы с электронной почтой.	1	Знакомятся с видеоматериалом. Составляют памятки с основными правилами пользования электронной почтой.
4.	Сообщения со взломанных аккаунтов.	1	Обсуждают в группе, какие методы вымогательства денег могут использовать злоумышленники для рассылок на ваш электронный адрес.
5.	Правила работы в социальной сети ВКонтакте.	2	Знакомятся с системой помощи при работе в социальной сети ВКонтакте. Регистрируются в социальной сети ВКонтакте.
6.	Компьютерные видеоигры.	1	Обсуждают в группе, как в компьютерных видеоиграх может быть встроено вымогательство денег.
7.	Правила работы в социальных сетях.	1	Обсуждают в группе, кто такие тролли в Интернете и как сними бороться, как защититься от нежелательных обращений. Знакомятся с кнопкой «Пожаловаться» в социальной сети ВКонтакте.
8.	Правила защиты от вирусов, спама, рекламы и рассылок.	1	Знакомятся с классификацией вирусов правилами защиты компьютера от вирусов, спама, рекламы и рассылок.
9.	Мошенничество в интернете. Правила защиты от негативных сообщений.	1	Обсуждают в группе, какие бывают виды сетевого мошенничества. Учатся правильно вести себя в проблемной ситуации.
10.	Правила общения в социальной сети.	1	Обсуждают в группе следующие вопросы:

			– Что недопустимо приобщении в социальной сети с незнакомцами? – Можно ли полностью доверять информации, которую размещают на своих страничках участники социальной сети? – Можно ли соглашаться на встречу в реальном мире с незнакомцами из социальной сети?
11.	Система помощи на страницах популярныхсоцсетей: ВКонтакте, Facebook, Одноклассники.	3	Изучают и обсуждают системы помощи на страницах популярных соцсетей. Учатся использовать только позитивный Интернет в познавательных целях.
12.	Как вести себя в социальных сетях?	1	Составляют памятки поведения в социальных сетях на тему информационной безопасности.
13.	Правила работы с поисковыми системами и анализ информации.	1	Обсуждают в группе, что такое пиратские сайты и почему они так называются.
14.	Ложная информация.	1	Обсуждают в группе, что такое ложная информация и как ее распознать.
15.	Правила ответственности за распространение ложной и негативной информации.	5	Знакомятся с законами, представленными на сайте «Безопасный Интернет для детей» Обсуждают в группе, как общество защищает детей в Интернете. Как обнаружить ложь и остаться правдивым в Интернете.
			Защита персональных данных. Детская безопасность в Интернете.
16.	Правила защиты от нежелательных сообщений и контактов.	1	Обсуждают в группе, какие угрозы подстерегают при общении с незнакомцами в социальных сетях.
17.	Правила вызова экстренной помощи. (2 часа)	2	Знакомятся с сайтом «Пространство безопасности. Школа первой помощи». Знакомятся с разделом «Телефоны первой помощи». Составляют памятку по основным сведениям, которые необходимо сообщить при вызове экстренных служб.
18.	Правила защиты устройств от внешнего вторжения.	1	Знакомятся с правилами подборки паролей.
Раздел «Путешествия по полезным ресурсам сети Интернет» (8 часов)			
19.	Полезные ресурсы в сети Интернет.	5	Знакомятся с сайтом Российская государственная детская библиотека. В разделе «Национальная электронная детская библиотека» знакомятся с каталогом книг, коллекцией диафильмов, архивом детских журналов. Выбирают писателя, знакомятся с его биографией. Знакомятся с сайтом Детская электронная библиотека.
20.	Средства работы в Интернете для людей с особыми потребностями.	2	Знакомятся с сайтом Всероссийского общества слепых. Знакомятся с сайтом Детское радио. Знакомятся с сайтом

			Звуковой учебник по информатике для начинающих. Знакомятся с сайтом Звуковой учебник по английскому языку для начинающих.
21.	Контрольное занятие.	1	Участвуют в викторине «Правила безопасности в сети Интернет»

9 класс

№	Тема	Кол-во часов	Характеристика основных видов деятельности учащихся
Раздел «Киберпространство» (29часов)			
1.	Киберпространство. Определение и структура киберпространства.	2	Знакомятся с понятием «киберпространство». Выделяют его структуру.
2.	История возникновения киберпространства.	1	Знакомятся с историей возникновения киберпространства.
3.	Этап современных информационных технологий.	1	Изучают этапы информационных технологий.
4.	Появление и развитие Интернет.	1	Изучают развитие сети Интернет.
5.	Базовые понятия в киберпространстве.	1	Знакомятся с понятием «доментное имя». Обсуждают доментные зоны.
6.	Браузеры.	1	Знакомятся с понятием «браузер» и его видами.
7.	Язык киберпространства: – Сайты и страницы. – Жанры гипертекста. – Процесс разработки сайта. – Классификация и назначение элементов сайта.	5	Знакомятся с понятиями: гипертекст, сетевой адрес, веб-страница, жанры текста, блог, веб-мастеринг, веб-мастер, контент-менеджмент, копирайтинг. Знакомятся с классификацией и назначением элементов сайта.
8.	Технические разделы сайта.	1	Знакомятся с блоками вспомогательного раздела сайта, обратной связи, навигационного раздела.
9.	Интернет 2020–2021 г.г. в мире и в России: статистика и тренды.	1	Обсуждают глобальную статистику интернета и соцсетей.
10.	Виртуальная реальность. Большой скачок.	1	Обсуждают развитие виртуальной реальности.
11.	Кибермиры.	2	Обсуждают тему киберразвития на примере Экзоскелета на службе парализованного человека. Обсуждают Интеллектуальное устройство Умный помощник «Робин», которое помогает незрячим людям ориентироваться в пространстве.
12.	Киберфизическая система.	3	Обсуждают, что такое искусственный интеллект и его развитие. Знакомятся с управлением дронами. Отвечают на вопросы: Где нельзя летать на дроне? В какие специальные зоны нельзя залетать? Нужна ли лицензия на полет?
13.	Киберобщество.	7	Обсуждают развитие социальных сетей. Обсуждают такие понятия, как кибероружие, мягкая сила, клиповое мышление. Знакомятся с такими понятиями, как психологические и алгоритмические операции. Обсуждают ключевые вопросы взаимодействия поколений в условиях информационного общества.

			Обсуждают вопросы обеспечения общественной безопасности в условиях киберсреды через раскрытие понятия «сетевые революции». Знакомятся с такими понятиями, как сетевые революции и инфантилизм. Решают вопрос о том, что знают о нас соцсети? Обсуждают такие вопросы, как: Что представляют из себя социальные сети? Чем они опасны и почему так привлекательны? Знакомятся с Киберугрозами. Знакомятся с таким понятием, как цифровой фашизм. Участвуют в викторине на сайте АЗБУКА КБ.
14.	Киберденьги.	1	Знакомятся с понятием Криптовалюты: золотая лихорадка цифрового века. Обсуждают вопросы: Как устроена технология блокчейн и каковы ее перспективы? Сколько криптовалют будет через 15 лет? Как, вообще, может существовать валюта, не привязанная к золотому запасу какой-либо страны?
15.	Кибермошенничество	1	Знакомятся и обсуждают Документ Уголовный Кодекс Российской Федерации Статья 187. Неправомерный оборот средств платежей –
Раздел «Онлайн-курс Академии Яндекс «Безопасность в Интернете»» (5 часов)			
16.	Онлайн курс Академии Яндекс «Безопасность в Интернете»	5 часов	Регистрируются на сайте Академии Яндекс Проходят онлайн-курс «Безопасность в Интернете», получают сертификат.

10 класс

№	Тема	Кол-во часов	Характеристика основных видов деятельности учащихся
Раздел «Киберкультура» (19 часов)			
1.	Киберкультура.	1	Знакомятся с понятием «киберкультура».
2.	Путешествие в закулисный мир Большого театра.	1	Знакомятся с роскошным интерьером Большого театра и узнают историю самого знаменитого театра страны.
3.	Московский планетарий.	2	Знакомятся с историй Московского планетария. Путешествуют по сайту Московского планетария. Виртуальная экскурсия по классическому музею Урании.
4.	От книги к гипертексту.	2	Работают в текстовом редакторе Word.
5.	Киберкнига. – Президент России гражданам школь-ного возраста. – Научная электронная библиотека «КиберЛенинка». – Российская госу-дарственная библиотека/Электронная библиотека.	8	Обсуждают российские книги с дополненной реальностью. Книги AR. – Обсуждают вопросы про Президента. Изучают Конституцию РФ. Изучают права детей. Изучают загадки Кремля. Изучают Президентскую библиотеку. – Изучают страницы научной электронной библиотеки. – Изучают страницы Российской государственной электронной библиотеки.

6.	Киберискусство.	2	Посещают онлайн Музей цифрового искусства в Токио. Изучают сайт Союзмультпарк, знакомятся с работой парка.
7.	Социальная инженерия.	1	Знакомятся с понятием «социальная инженерия», обсуждают её важность в современном мире.
8.	Классификация угроз социальной инженерии.	1	Обсуждают Федеральный закон о персональных данных.
9.	Меры безопасности при использовании банковских карт.	1	Изучают правила безопасности при использовании банковских карт.
Раздел «Киберугрозы» (4 часа)			
1.	Кибервойны.	1	Обсуждают развитие технологий искусственного интеллекта.
2.	Киберпреступность и информационная преступность.	1	Обсуждают виды угроз информационной безопасности.
3.	Запрещенные и нежелательные сайты.	1	Знакомятся с Федеральным законом №149-ФЗ «Об информации, информационных технологиях и о защите информации».
4.	Обзор антивирусного ПО.	1	Знакомятся с антивирусными программами.
Раздел «Профориентация» (11 часов)			
1.	Рынок труда.	1	Знакомятся с основными сферами профессиональной деятельности на современном рынке труда.
2.	Среднее специальное учебное заведение (ссуз).	1	Знакомятся с видами и типами среднего профессионального образования. Изучают правила поступления.
3.	Учебные заведения среднего профессионального образования г.Армавира	2	Знакомятся с местными учебными заведениями, с их структурой образования. Знакомятся со специальностями на базе средних профессиональных образовательных учреждений г.Армавира.

			тельных учреждений РФ.
6.	Моя профессия.	1	Определяют значимость будущей профессии.

8.Описание материально-технического обеспечения.

Для успешной реализации программы курса для обучающихся с нарушениями слухатребуется материально-техническое обеспечение:

- технические средства обучения и воспитания (ИКТ);
- цифровые и электронные образовательные и воспитательные ресурсы;
- демонстрационные пособия;
- дополнительные материалы (сайты, видеоматериалы);
- мультимедийные презентации, авторские презентации.

СОГЛАСОВАНО
Протокол заседания
методического объединения воспитателей среднего и старшего звена
ГКОУ школы-интерната №2
г.Армавира
от 29.08.2023г. №1
/Ялыкина У.М./

СОГЛАСОВАНО
Заместитель директора по ВР
ГКОУ школы-интерната №2
г.Армавира
/Н.В.Даньшина/
29.08.2023года

РЕЦЕНЗИЯ
на методический материал «Правила безопасного поведения в Интернет-пространстве» к рабочей программе факультатива «Информационная безопасность» воспитателя ГКОУ школы-интерната №2 города Армавира Ядыкиной Ульяны Михайловны

Представленный на рецензию методический материал могут использовать педагоги специальных коррекционных учреждений для обучающихся с нарушениями слуха во внеурочной деятельности и на факультативных занятиях по курсу «Информационная безопасность». Данные материалы направлены на систематизацию знаний обучающихся с нарушениями слуха полученные при изучении курса; на профилактику интернет-зависимости, националистических проявлений в молодежной среде и устранение риска вовлечения подростков в противоправную деятельность. Данный методический материал разработан в помощь педагогам 5-10 классов обучающихся с нарушениями слуха для реализации специальных условий с учетом их особых образовательных потребностей, в том числе обеспечивающий коррекцию нарушений развития.

Основная цель данного методического материала - обеспечить состояние защищенности детей с ОВЗ, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

Представленный материал построен в соответствии с последними требованиями ФГОС основного общего образования (приказ Министерства просвещения РФ от 31.05.2021г. № 287) и ФАОП ООО для обучающих с ОВЗ (приказ Министерства просвещения РФ от 24 ноября 2022 г. №1025).

Методический материал воспитателя Ядыкиной У.М. соответствует требованиям Министерства образования РФ, специфике данного учреждения. Целесообразно рекомендовать его к использованию в специальных коррекционных образовательных учреждениях для детей с нарушениями слуха во внеурочной деятельности.

Удостоверяю подпись
Специалист по персоналу
отдела молодежной политики
управления кадровой политики
Министерства просвещения
и воспитания Ставропольского края

Рецензент:
к.псх.н., доцент, кафедры
ССПиП ФГБОУ ВО «АГПУ» А.М. Дохоян

Государственное казенное общеобразовательное учреждение Краснодарского края
специальная (коррекционная) школа-интернат № 2 г. Армавира
(ГКОУ школа-интернат № 2 г. Армавира)

МЕТОДИЧЕСКИЙ МАТЕРИАЛ

К РАБОЧЕЙ ПРОГРАММЫ ФАКУЛЬТАТИВА ПО КУРСУ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

«ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ»

Составитель:
воспитатель
Ядыкина Ульяна
Михайловна

Армавир,2023 год

Содержание.

1. Аннотация.

Представленный методический материал могут использовать учителя специальных коррекционных учреждений для обучающихся с нарушениями слуха во внеурочной деятельности и воспитатели на факультативных занятиях по курсу «Информационная безопасность». Данные материалы направлены на систематизацию знаний обучающихся с нарушениями слуха полученные при изучении курса; на профилактику интернет-зависимости, националистических проявлений в молодежной среде и устранение риска вовлечения подростков в противоправную деятельность.

2. Пояснительная записка.

Сборник методического материала соответствует требованиям Федерального государственного образовательного стандарта основного общего образования (приказ Министерства просвещения РФ от 31.05.2021г. № 287) и ФАОП ООО для обучающих с ОВЗ (приказ Министерства просвещения РФ от 24 ноября 2022 г. №1025).

Данный методический материал разработан в помощь педагогам 5-10 классов, обучающихся с нарушениями слуха для реализации специальных условий с учетом их особых образовательных потребностей, в том числе обеспечивающая коррекцию нарушений развития.

Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

В Интернете, как и в реальной жизни, обучающихся с ОВЗ подстерегают опасности: доступность нежелательного контента в социальных сетях, обман и вымогательство денег, платные СМС на короткие номера, пропаганда насилия и экстремизма, игромания и интернет-зависимость, склонение к суициду и т. п.

Задача педагогов в связи с имеющимися рисками состоит в том, чтобы указать на эти риски, предостеречь от необдуманных поступков, сформировать у учащихся навыки критического отношения к получаемой в Интернете информации, воспитать культуру безопасного использования Интернет. Также следует обратить внимание на гигиенические требования, которые необходимо соблюдать при работе с компьютером.

3. Основная часть.

Интернет уже давно стал незаменимым помощником современного человека. Всемирная сеть - является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Именно поэтому дети с ОВЗ активно пользуются Интернетом, а зачастую проводят в Сети даже больше времени, чем взрослые. Обучающиеся с нарушениями слуха осваивают сервисы мгновенных сообщений и интернет телефонию, общаются на форумах и в чатах, каждый день узнают много новой увлекательной и образовательной информации.

Однако не стоит забывать, что Интернет может быть не только средством для обучения, отдыха или общения с друзьями, но – как и реальный мир – Сеть тоже может быть опасна.

Наиболее часто встречающиеся угрозы при работе в Интернет:

1. Угроза заражения вредоносным программным обеспечением (ПО). Для распространения вредоносного ПО и проникновения в компьютеры используется почта, компакт-диски, дискеты и прочие сменные носители, или скачанные из сети Интернет файлы;

2. Доступ к нежелательному содержимому. Это насилие, наркотики, страницы подталкивающие к самоубийствам, отказу от приема пищи, убийствам, страницы с националистической идеологией. Независимо от желания пользователя, на многих сайтах отображаются всплывающие окна, содержащие подобную информацию;

3. Контакты с незнакомыми людьми с помощью чатов или электронной почты. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. Выдавая себя за сверстника, они могут выведывать личную информацию и искать личной встречи;

4. Поиск развлечений (например, игр) в Интернете. Иногда при поиске нового игрового сайта можно попасть на карточный сервер и проиграть большую сумму денег.

5. Неконтролируемые покупки.

Компьютерные вирусы.

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. Вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через Интернет.

Сети WI-FI.

Wi-Fi — это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «WirelessFidelity», который переводится как «беспроводная точность».

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высший звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в Интернет. Но многие эксперты считают, что общедоступные Wi-Ficети не являются безопасными.

Социальные сети.

Социальные сети активно входят в нашу жизнь, подростки с ОВЗ «живут» там постоянно. Ребята с нарушениями слуха не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Электронные деньги

Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно, однако в России они функционируют и о них уже прописано в законе, где их разделяют на несколько видов – анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в не анонимных идентификации пользователя является обязательной.

Электронная почта.

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Мобильный телефон.

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Online игры.

Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции. В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Фишинг или кража личных данных.

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в Интернет, и продолжают заниматься кражей. Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей.

4. Заключение.

Безопасность в сети Интернет в свете быстрого развития информационных технологий резко повышает потребность в воспитании у обучающихся культуры информационной безопас-ности в целях предотвращения негативных последствий массово-го использования Интернета детьми и их защиты от агрессивной и противоправной информации.

Особой потребностью в воспитании культуры информационной безопасности нуждаются обучающиеся с нарушениями слуха, так как это не только нарушает социальную адаптацию человека, но влияет на его психическое развитие.

ПРИЛОЖЕНИЕ

1. Гигиенические требования при работе с компьютером.

- школьникам среднего и старшего возраста можно проводить перед монитором до двух часов в день, устраивая 10-15-минутные перерывы каждые полчаса;
- лучше работать за компьютером в первой половине дня;
- комната должна быть хорошо освещена;
- при работе за компьютером следить за осанкой, мебель должна соответствовать росту;
- расстояние от глаз до монитора – 60 см;
- периодически делать зарядку для глаз.

2. **Безопасность в сети Интернет.**

Памятка по безопасности в сети Интернет.

Никогда	Всегда
Никогда не оставляй встреченным в Интернете людям свой номер телефона, домашний адрес или номер школы без разрешения родителей.	Всегда будь внимательным, посещая чаты. Даже если в чате написано, что он только для детей, нельзя точно сказать, что все посетители действительно являются твоими ровесниками. В

	чатах могут сидеть взрослые, пытающиеся тебя обмануть.
Никогда не отправляй никому свою фотографию, не посоветовавшись с родителями.	Всегда спрашивай у родителей разрешения посидеть в чате.
Никогда не договаривайся о встрече с интернет-знакомыми без сопровождения взрослых. Они не всегда являются теми, за кого себя выдают. Встречайся только в общественных местах.	Всегда покидай чат, если чье-то сообщение вызовет у тебя чувство беспокойства или волнение. Не забудь обсудить это с родителями.
Никогда не открывай прикрепленные к электронному письму файлы, присланные от незнакомого человека. Файлы могут содержать вирусы или другие программы, которые могут повредить всю информацию или программное обеспечение компьютера.	Всегда держи информацию о пароле при себе, никому его не говори.
Никогда не отвечай на недоброжелательные сообщения или на сообщения с предложениями, всегда рассказывай родителям, если получил таковые.	Всегда помни, что если кто-то сделает тебе предложение, слишком хорошее, чтобы быть правдой, то это, скорее всего, обман.
	Всегда держись подальше от сайтов "только для тех, кому уже есть 18". Такие предупреждения на сайтах созданы специально для твоей же защиты. Сайты для взрослых также могут увеличить твой счет за Интернет.

3. Компьютерные вирусы. Методы защиты от вредоносных программ:

Памятка по защите от компьютерных вирусов.

1. Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
2. Постоянно устанавливай почти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;

4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничь физический доступ к компьютеру для посторонних лиц;
6. Используй внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников;
7. Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

4.Сети WI-FI.

Советы по безопасности работе в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
4. Не используй публичный WI-FIдля передачи личных данных, например, для выхода в социальные сети или в электронную почту;
5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
6. В мобильном телефоне отключи функцию «Подключение к Wi-Fiавтоматически». Не допускай автоматического подключения устройства к сетям Wi-Fiбез твоего согласия.

5. Социальные сети.

Советы по безопасности в социальных сетях

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
3. Защищай свою репутацию — держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

6. **Электронные деньги**.

Основные советы по безопасной работе с электронными деньгами.

1. Надо выбрать правильный почтовый сервис. В Интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;
6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

7. Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

7. **Электронная почта.**

Основные советы по безопасной работе с электронной почтой.

1. Надо выбрать правильный почтовый сервис. В Интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;
6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
7. Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

8. **Мобильный телефон.**

Основные советы для безопасности мобильного телефона:

1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
3. Необходимо обновлять операционную систему твоего смартфона;
4. Используй антивирусные программы для мобильных телефонов;
5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;
7. Периодически проверяй какие платные услуги активированы на твоем номере;
8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

9. Online игры.

Основные советы по безопасности твоего игрового аккаунта.

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
2.Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
3.Не указывай личную информацию в профайле игры;
4.Уважай других участников по игре;

5.Не устанавливай неофициальные патчи и моды;
6.Используй сложные и разные пароли;
7.Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

10. Фишинг или кража личных данных.

Основные советы по борьбе с фишингом.

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установи надежный пароль (PIN) на мобильный телефон;
6. Отключи сохранение пароля в браузере;
7. Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

4.3 Повышение квалификации по профилю (направлению) деятельности

Образовательное частное учреждение

высшего образования

«Армавирский социально-психологический институт»

УДОСТОВЕРЕНИЕ

О ПОВЫШЕНИИ КВАЛИФИКАЦИИ

232415274192

Документ о квалификации

Регистрационный номер

984

Город

Армавир

Дата выдачи

30 мая 2022 года

Настоящее удостоверение свидетельствует о том, что

Ядыкина Ульяна Михайловна

прошел(а) повышение квалификации в (на)

Образовательном частном учреждении

высшего образования

«Армавирский социально-психологический институт»

по дополнительной профессиональной программе

Психолого-педагогические особенности воспитательной коррекционной работы, а также ее дистанционной формы при преподавании английского языка для глухих и слабослышащих обучающихся, а также глухих и слабослышащих, имеющих ЗПР, УО в соответствии с ФГОС НОО, ООО, СОО

в объёме 72 часа

М.П.

Руководитель Д.Н. Недбаев

Секретарь Ж.А. Сорокина

РОССИЙСКАЯ ФЕДЕРАЦИЯ

Министерство просвещения
Российской Федерации
федеральное государственное бюджетное образовательное
учреждение высшего образования
«Армавирский государственный
педагогический университет»

УДОСТОВЕРЕНИЕ

О ПОВЫШЕНИИ КВАЛИФИКАЦИИ

Серия 23У №1767005893

Документ о квалификации

Регистрационный номер
1191/21

Город
Армавир

Дата выдачи
11.07.2021 г.

Настоящее удостоверение свидетельствует о том, что

Ядыкина

Ульяна Михайловна

прошел (а) повышение квалификации в
федеральном государственном бюджетном образовательном
учреждении высшего образования
«Армавирский государственный педагогический
университет»

по дополнительной профессиональной программе
"Специфические средства коммуникаций неслышащих. Дактилология и русский жестовый язык"
16.06.2021 г. - 10.07.2021 г.

в объёме
144 часов

Руководитель Ю.П.Ветров

Секретарь Д.С.Шевелева

РОССИЙСКАЯ ФЕДЕРАЦИЯ

Министерство просвещения
Российской Федерации
федеральное государственное бюджетное образовательное
учреждение высшего образования
«Армавирский государственный
педагогический университет»

УДОСТОВЕРЕНИЕ

О ПОВЫШЕНИИ КВАЛИФИКАЦИИ

Серия 23У №1767006076

Документ о квалификации

Регистрационный номер

1345/21

Город
Армавир

Дата выдачи

07.10.2021 г.

Настоящее удостоверение свидетельствует о том, что

Ядыкина

Ульяна Михайловна

прошел (а) повышение квалификации в
федеральном государственном бюджетном образовательном
учреждении высшего образования
«Армавирский государственный педагогический
университет»

по дополнительной профессиональной программе

"Обучение педагогических работников навыкам оказания первой помощи"

22.09.2021 г. - 06.10.2021 г.

в объёме

72 часов

Руководитель Ю.П.Ветров

Секретарь Д.С.Шевелева