**Программа классных часов по кибербезопасности для обучающихся МБОУ «Зайчиковская ОШ» 1-9 классов**

**1-4 классы**

|  |  |
| --- | --- |
| **Формы проведения**  **Ссылки на материалы** | **Рекомендации и комментарии по материалам программы** |
| Классный час: Урок Цифры на тему «Кибербезопасность будущего» в рамках Всероссийского образовательного проекта в сфере цифровой экономики «Урок Цифры» (рекомендован к проведению с 15 января по 4 февраля 2024 г.)  Режим доступа: <https://урокцифры.рф/> | Урок Цифры по теме «Кибербезопасность будущего» представляет собой видеолекцию плюс тренажер и предназначен для обучающихся 3-4 классов. Предложенные материалы информируют ученика и затем тренируют умения ребенка по защите гаджетов, используемых в системе «Умный дом». Последовательность изучения: обязательно сначала видеолекция, затем тренажер, в котором ученику предлагается помочь героям обезопасить умный дом и даже умный город. На конкретном примере ребенок узнает, как противостоять самым разным кибератакам, которые нас могут ожидать в будущем и встречаются уже сейчас.  Отмечаем следующие особенности материалов:   * в материалах встречаются и частично разъясняются малознакомые обычному школьнику понятия (интернет вещей, уязвимости, патчи, майнинг, дедос-зловреды и многие другие); * при самостоятельной работе с тренажером ученик должен обладать уверенными пользовательскими навыками; * пользование системой «Умный дом» и гаджетами, подключенными к данной системе, по мнению разработчиков урока, является обыденным явлением в жизни ребенка, изучающего материалы.   Для эффективной работы с данными материалами многим обучающимся потребуются дополнительная помощь и разъяснения взрослых.  Материалы Урока Цифры по теме «Кибербезопасность будущего» являются небольшой частью масштабной программы по тренировке навыков киберзащиты в современном мире.  Дополнительно педагогам можно использовать на этом сайте материалы проекта [Цифровой ликбез](https://digital-likbez.datalesson.ru/). |
| Классный час: викторина «Безопасность пользователей в сети Интернет»  Режим доступа:  <https://quiz.safe-surf.ru/> | Викторина предназначена для учеников 4 классов. Вопросы построены на основе наиболее распространённых ошибок людей, использующих сеть Интернет. Викторина поможет понять, какие ситуации представляют потенциальную опасность.  Вопросы содержат специальные термины, достаточно сложные на начальном этапе, но, если ученик ошибается, педагог объяснит, как поступить правильно.  Пройти викторину можно в двух режимах: «Битва за рекорд» и «Развлекательный». Первый – соревновательный – для сравнивания знаний участника в сфере информационной безопасности с знаниями других участников викторины. Второй – обучающий – нацелен на разбор предлагаемых ситуаций. |
| Классные часы-практикумы «Правила кибербезопасности»  Ресурс «Российская электронная школа», темы возрастной классификации «6+»): «Максимальный репост», «Ты не один», «Лучший подарок»  Режим доступа:  <https://resh.edu.ru/page/cyber-project> | Предложенные материалы представляют собой профессиональные видеоролики, раскрывающие острые социальные проблемы, возникающие вследствие неправильных действий детей в среде Интернет. Видеоролики несут сильную эмоциональную окраску, наполнены яркой содержательной картиной и музыкой.  В роликах «Максимальный репост», «Лучший подарок», «На игре» раскрыты сюжеты, близкие детям младшего школьного возраста: общение в мессенджерах и социальных сетях и последствия взаимодействия с мошенниками. В ролике «Ты не один» показан пример школьной травли с использованием возможностей сети.  Рекомендуется совместный просмотр и обсуждение сюжета со взрослыми.  Возрастные категория видеороликов следующие: «Максимальный репост» – 1-2 класс, «Ты не один» – 3-4 класс, «Лучший подарок» – 3-4 класс, «На игре» – 4 класс. |

**5-6 классы**

|  |  |
| --- | --- |
| **Формы проведения**  **Ссылки на материалы** | **Рекомендации и комментарии по материалам программы** |
| Классный час: Урок Цифры на тему «Кибербезопасность будущего» в рамках Всероссийского образовательного проекта в сфере цифровой экономики «Урок Цифры» (рекомендован к проведению с 15 января по 4 февраля 2024 г.)  Режим доступа:  <https://урокцифры.рф/> | Урок Цифры по теме «Кибербезопасность будущего» представляет собой видеолекцию, методические материалы для учителя и 3 совершенно разных тренажера для обучающихся разных возрастных категорий (1-4, 5-8 и 9-11 классов). Видеолекция, методические материалы для проведения занятия и сам тренажер доступны на сайте урокцифры.рф.  Тематика урока посвящена основным правилам кибербезопасности. Средним классам предложена тема «Носимые устройства», старшим – «Система «Умный город».  Формат урока – урок с компьютерной поддержкой и доступом в интернет.  Школьники узнают, что такое интернет вещей, как обезопасить умный дом, защищать данные на смартфонах и противостоять самым разным кибератакам, в том числе тем, что реализуются с использованием продвинутых технологий; познакомятся с многообразием профессий в ИТ и специалистами, которые уже сегодня разрабатывают подходы и решения для защиты различных устройств, чтобы сделать современный цифровой мир безопаснее.  По сюжету герои попадают в симуляцию будущего – в 2050 год. Задания и сценарии различаются для учеников младших (1-4), средних (5-8) и старших (9-11) классов. Несмотря на то, что действие происходит в далеком будущем, в выдуманных мирах, задания носят вполне практический характер и учат, как защищаться от киберугроз сегодняшнего дня. Например, учащимся расскажут, какие устройства являются носимыми, а какие относятся к обычным гаджетам, где можно скачать защитное решение для своего устройства.  Школьникам 5-8 классов рекомендуется выбирать уровень «Для опытных специалистов». |
| Классный час: викторина «Безопасность пользователей в сети Интернет»  Режим доступа:  <https://quiz.safe-surf.ru//> | Викторина построена по аналогии с игрой «Своя игра», имеет поле, состоящее из 35/25 вопросов, в зависимости от уровня. У каждого вопроса есть свой вес (100, 200, 300, 400, 500 баллов).  Представлены вопросы разной тематики: актуальные угрозы в Интернете, защита домашнего ПК, защита мобильных устройств, безопасная работа с e-mail, безопасность в социальных сетях и мессенджерах, безопасность при поиске и серфинге в Интернете, онлайн-банкинг и Интернет-коммерция.  Пройти викторину можно в двух режимах: «Битва за рекорд» и «Развлекательный».  Первый – соревновательный – подойдёт, для сравнивания знаний участника в сфере информационной безопасности с знаниями других участников викторины. Второй — обучающий – нацелен на разбор предлагаемых ситуаций.  Викторина содержит множество специальных терминов, при ошибочном ответе дается разъяснение.  Целесообразно использовать не только в 5-6 классах, но и в 7-9. |
| Классный час: Цифровой квест «Безопасность в сети Интернет»  Режим доступа:  <https://learningapps.org/3391444> | 1. Квест создан в сервисе для создания обучающих игр и игровых упражнений LearningApps. Нацелен на закрепление знаний о правилах безопасного поведения в сети Интернет в процессе игровой деятельности. Представлены обучающие видеоролики и различные задания: на сортировку терминов, сопоставление понятия с определением, решение ситуационных задач, тестовые задания. Квест состоит из 5 этапов. 2. Каждый этап посвящен определенной тематике: 3. Основные понятия информационной безопасности; 4. Как обнаружить ложь и остаться правдивым в Интернете; 5. Развлечения и безопасность в Интернете; 6. Остерегайся мошенничества в Интернете; 7. Угрозы сети. 8. Веб-квест «Интернет и безопасность в нем» является интерактивной формой, которая способна увлечь детей, погрузить их в мир приключений, дать возможность продемонстрировать смекалку, талант и получить удовольствие от участия. |
| Классный час «Как пользоваться мобильной связью без вреда своему здоровью»  Режим доступа:  <https://цпмсс.рф/files/biblioteka/КИБЕРУРОКИ_2022_Методические_разработки.pdf> | Урок посвящен теме влияния на организм мобильного телефона.  Цель: Сформировать у обучающихся 5-6 классов понятие рационального использования средств мобильной связи не причиняя вред физиологическому, эмоциональному и психологическому здоровью.  Задачи:  1. Повысить уровень информированности о сущности безопасного использования мобильного телефона;  2. Содействовать развитию навыков оценки и самооценки степени опасности бесконтрольного пользования мобильным телефоном;  3. Мотивировать на более безопасное для здоровья использование мобильного телефона;  Вначале урока с обучающимся проводится анкетирование, а затем приводится статистика и результаты исследования о воздействии телефонов на организм школьников-подростков. Согласно статистике операторов сотовой связи:  - около 70% пользователей разговаривают по телефону более 30 минут в день;  - 30% людей имеют по 2 сотовых и регулярно их используют;  - 40% наших сограждан на ночь кладет телефон на расстояние менее 0,7 метра от головы, а ведь даже не звонящий аппарат постоянно связывается с базовой станцией;  - только 20% пользователей знают, что влияние мобильного телефона на человека может быть чрезвычайно вредным.  Согласно последним фактам сотовые телефоны снижают иммунитет, изменяют психику и увеличивают биологический возраст человека. И это уже не просто «страшилка»: медики утверждают, что по степени опасности сотовые и радиотелефоны можно смело приравнять к сигаретам и алкоголю. Длительное облучение электромагнитным излучением приводит к нарушению всех основных функций мозга: мышления, памяти, внимания. Исследователи изучали состояние хрусталика глаза, а также нервной системы. Выяснилось, что мобильные телефоны вызывают невосстанавливаемые изменения в обследуемых органах и подкорковых структурах головного мозга. А биологический возраст активных пользователей превышает календарный в среднем на 6-8 лет.  Ребятам предлагается провести обсуждение по группам и разработать памятки со своими правилами безопасного пользования мобильным телефоном.  Правила:  1. Ограничить время и частоту использования сотового телефона;  2. Стараться по возможности не использовать телефон в тех местах, где наблюдается плохой приём (лифт, подземные помещения, транспорт и т. д.), так как при плохом приёме мобильный телефон пытается найти антенну-передатчик, и из-за этого его излучение (свойства и воздействия которого на человека до сих пор ещё в полной мере не изучены) многократно усиливается;  3. Реже использовать мобильный телефон в закрытых помещениях (машина, дом, лифт), так как излучаемые им волны могут отражаться стенами и покрытиями, что в несколько раз усиливает облучение;  4. Имейте в виду, что беспроводной способ передачи данных от одного мобильника к другому, разработанный под маркой Bluetooth, прибавляет мобильному телефону дополнительную силу излучения;  5. Не прикладывайте мобильный телефон к уху в тот момент, когда он находится в процессе поиска оператора сети (это бывает при самом включении и при плохом приёме). В этот момент он излучает больше всего, вредит, так сказать, по максимуму;  6. И, наконец, избавьтесь от пагубной привычки спать рядом с сотовым телефоном (тем более класть включённый, работающий (а, значит, постоянно излучающий!!!) мобильник под ПОДУШКУ!) А если вы привыкли использовать телефон в качестве будильника, то лучше отложить его в дальний угол вашей спальни. |

**7-9 классы**

|  |  |
| --- | --- |
| **Формы проведения**  **Ссылки на материалы** | **Рекомендации и комментарии по материалам программы** |
| Классный час: Урок Цифры на тему «Кибербезопасность будущего» в рамках Всероссийского образовательного проекта в сфере цифровой экономики «Урок Цифры» (рекомендован к проведению с 15 января по 4 февраля 2024 г.)  Режим доступа:  <https://урокцифры.рф/> | Урок Цифры по теме «Кибербезопасность будущего» представляет собой видеолекцию, методические материалы для учителя и 3 совершенно разных тренажера для обучающихся разных возрастных категорий (1-4, 5-8 и 9-11 классов). Видеолекция, методические материалы для проведения занятия и сам тренажер доступны на сайте урокцифры.рф.  Тематика урока посвящена основным правилам кибербезопасности и проблемам в этой области. Средним классам предложена тема «Носимые устройства», старшим «Система «Умный город».  Формат урока - урок с компьютерной поддержкой и доступом в интернет.  Школьники узнают, что такое интернет вещей, как обезопасить умный дом, защищать данные на смартфонах и противостоять самым разным кибератакам, в том числе тем, что реализуются с использованием продвинутых технологий; познакомятся с многообразием профессий в ИТ и специалистами, которые уже сегодня разрабатывают подходы и решения для защиты различных устройств, чтобы сделать современный цифровой мир безопаснее.  По сюжету герои попадают в симуляцию будущего – в 2050 год. Задания и сценарии различаются для учеников младших (1-4), средних (5-8) и старших (9-11) классов. Несмотря на то, что действие происходит в далеком будущем, в выдуманных мирах, задания носят вполне практический характер и учат, как защищаться от киберугроз сегодняшнего дня. Например, учащимся расскажут, какие устройства являются носимыми, а какие относятся к обычным гаджетам, где можно скачать защитное решение для своего устройства.  Школьникам 5-8 классов рекомендуется выбирать уровень «Для опытных специалистов», для 9-11 классов уровень «Продвинутый пользователь». |
| Классные часы с просмотром роликов и обсуждением, диспутом, беседой  Ресурс «Российская электронная школа», темы возрастной классификации «12+»; «На игре»  Режим доступа:  <https://resh.edu.ru/page/cyber-project> | Для обучающихся 7-9 классов рекомендуется выбирать материалы категории «12+».  На странице КИБЕРБЕЗОПАСНОСТЬ ДЛЯ ДЕТЕЙ И ВЗРОСЛЫХ представлен видеосюжет о том, как девочка Варя вступает в опасную сетевую игру для подростков. Ни одноклассники, ни учителя, ни родители не замечают, что происходит с девочкой. Равнодушие окружающих едва не стало причиной трагедии.  В конце ролика даются советы, как не попасть в подобную ситуацию или выйти из нее.  Видеоролики несут сильную эмоциональную окраску, наполнены яркой содержательной картиной и музыкой. Рекомендуется совместный просмотр и обсуждение сюжета со взрослыми. |
| Классные часы-практикумы «Правила кибербезопасности»  Режим доступа:  <https://цпмсс.рф/files/biblioteka/КИБЕРУРОКИ_2022_Методические_разработки.pdf> | Цель классных часов: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.  В сборнике представлено большое количество разработок классных часов для разных возрастных категорий.  **Киберурок «Интернет-сообщества, виртуальные друзья»**  Любая социальная сеть – это база, в которую вы вносите персональные данные. При этом многие пользователи слишком откровенны, они с охотой публикуют полную информацию о себе.  Обучающимся предлагается поработать в группе. Каждая группа разбирает кейс-задание по правилам безопасного поведения в Интернете.  **Киберурок «Безопасный интернет. Как правильно себя вести в сети»**  В ходе урока обучающиеся учатся находить плюсы и минусы виртуальной паутины, аргументировать свою точку зрения.  Сделана подборка ресурсов с видеоматериалами «Что можно? Что нельзя? К чему надо относиться осторожно?».  **Киберурок «Урок по безопасности в сети Интернет»**  Ценность урока заключается в наличии памяток с советами по безопасной работе в общедоступных сетях Wi-Fi, в социальных сетях, с электронными деньгами, по безопасности мобильного телефона и игрового аккаунта, по борьбе с кибербуллингом и защите цифровой репутации.  **Киберурок «Безопасность учащихся в сети Интернет»**  Дается классификация угроз: онлайн и оффлайн.  К онлайн-угрозам относятся различные категории компьютерных вредителей и вирусов:  - программы-шпионы (будут отслеживать все действия пользователя на компьютере, вводимую информацию с целью ее похищения (пароли, логины, номера кредитных карт));  - винлокеры (программы, которые перекрывают картинкой весь экран и предлагаю заплатить определенную сумму от 100 до 500 рублей, чтобы разблокировать компьютер. Очень часто винлокеры используют картинку порнографического содержания и угрозы сообщить о пользователе в полицию, как о любителе запрещенного порно, когда он таковым не является);  - подписка на «премиальные» номера для загрузки какой-нибудь бесплатной программу, типа сервиса для обмена сообщениями;  - фишинг - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей;  - попадание в базы рассылки спама (если электронный адрес появится в открытом доступе).  Онлайн-угрозы могут просочиться на компьютер во время путешествия по просторам социальных сетей. Для этого порой достаточно нажать на ссылку, содержащуюся в письме от «мнимого» друга.  Онлайн-угрозы могут также навредить репутации.  Офлайн-угрозы – самый опасный вид угроз, может принести ущерб не только имуществу, но и жизни. К ним относятся предложения о встрече от неизвестных «друзей», телефонный шантаж, мошенничество, вымогательство и даже ограбление квартиры или кража другого имущества (например, при регистрации в социальной сети и составлении личного профайла предлагается внести информацию о своем годе рождение, номер телефона, адрес электронной почты, адрес проживания и работы).  Для защиты необходимо использовать «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр, модули для полной защиты вашего компьютера. |
| Классный час: видеоролики для совместного обсуждения «Цифровой ликбез»  Режим доступа:  <https://digital-likbez.datalesson.ru/?ysclid=lq9ao7tgwg493635375> | ЦИФРОВОЙ ЛИКБЕЗ – просветительский проект, который поможет повысить цифровую грамотность и узнать больше о кибербезопасности в сети.  Видеоролики для детей и взрослых от ведущих цифровых компаний-лидеров: VK, Благотворительный фонд Сбербанка «Вклад в будущее», «Почта России», «Лаборатория Касперского».  Видеоролики рекомендуется смотреть обучающимся с учителем или родителями в целях уточнения непонятных слов, осмысления полученной информации, совместного обсуждения. Много нового для себя могут узнать и взрослые.  Рекомендуются для обучающихся начальной школы (1,2,3,4 классы) и 5-6 классов, т.к. информация изложена в упрощенном виде, в форме мультипликации, обучающимся 7-9 классов будет не интересно. |