9 КЛАСС ОБЗР

Цифровая среда — конспект урока

Автор Глеб Беломедведев

ФЕВ 2, 2025 19 фото Время прочтения: 35 минут(ы)

Просмотров: 5

#безопасность, #видео, #вирус, #возможности, #интеллект-карта, #интересные факты, #Интернет, #карта памяти, #кроссворд, #ментальная карта, #метод, #облако слов, #образование, #полезные советы, #презентация, #ресурсы, #риск, #сеть, #среда, #таблица, #телефон, #тесты, #технологическая карта, #угроза, #цифровая, #чек-лист

Содержание [Скрыть]

Поиск

Поиск

ИНТЕРЕСНОЕ

КОНСПЕКТЫ УРОКОВ

Конспекты уроков для учителя
Английский язык
Астрономия
10 класс
Библиотека
Биология
5 класс
6 класс
7 класс
8 класс
География
5 класс
6 класс
7 класс
8 класс
9 класс
10 класс
Геометрия
Директору и завучу школы
Должностные инструкции
ИЗО
Информатика
История

Цифровая среда — ее возможности и риски. Общие принципы безопасности в цифровой среде — конспект урока ОБЗР (Основы безопасности и защиты Родины)

Вступление

> ***Вы когда-нибудь задумывались, почему подростки готовы провести целый день, уткнувшись в экран гаджета? А что происходит, когда вместо ожидаемого общения с друзьями они сталкиваются с агрессией или мошенничеством? Этот конспект раскроет не только секреты безопасного поведения в виртуальном мире, но и предоставит готовые материалы для эффективного занятия. Здесь вы найдете подробную технологическую и интеллект-карту, кроссворд, бесплатную презентацию, тесты и рабочий лист, которые сделают ваше мероприятие незабываемым.***

Классный руководитель
5 класс
6 класс
7 класс
8 класс
9 класс
10 класс
11 класс
Профориентационные уроки
Математика
Музыка
Начальная школа
ОБЗР
8 класс
9 класс
10 класс
11 класс
Обществознание
Право
Психология
Русская литература
Русский язык
Технология (Труды)
Физика
Физкультура
Химия
Экология
Экономика
Копилка учителя
Сценарии школьных праздников

Выберите похожие названия

- Методическая разработка: «Безопасность в цифровом мире: возможности и угрозы»
- Интегрированное занятие: «Информационная гигиена современного подростка»
- Практикум по цифровой безопасности: «Я и виртуальный мир»
- Урок-исследование: «Цифровые технологии: правила выживания»

Возраст учеников

14-15 лет

Класс

9 класс

Календарно-тематическое планирование

КТП по ОБЗР 9 класс

Модуль

Модуль № 10 «Безопасность в информационном пространстве»

УМК (Учебно-методический комплекс)

[укажите название своего УМК по которому Вы работаете]

Учебник

[укажите название своего учебника]

Дата проведения

[укажите дату проведения]

Длительность

45 минут (1 академический час)

Вид

Комбинированный

Тип

Изучение нового материала с элементами практической работы

Форма проведения

Урок-практикум с элементами дискуссии

Цель

- Сформировать у обучающихся представление о безопасном поведении в цифровой среде и развить навыки противодействия информационным угрозам

Задачи

- **Обучающая:** сформировать представление о цифровой среде, её возможностях и рисках; познакомить с основными принципами безопасного поведения в цифровом пространстве
- **Развивающая:** развить критическое мышление и навыки анализа информационных угроз
- **Воспитательная:** воспитать ответственное отношение к личной информационной защищённости

Универсальные учебные действия (УУД)

- **Личностные УУД:** формирование ответственного отношения к собственной информационной защите
- **Регулятивные УУД:** развитие умения планировать свое поведение в интернет-среде
- **Познавательные УУД:** освоение способов безопасного использования цифровых технологий
- **Коммуникативные УУД:** развитие навыков безопасного сетевого общения
- **Метапредметные УУД:** формирование культуры безопасного поведения в интернет-среде

Методические приёмы, педагогические методы, технологии обучения

- Кейс-метод
- Анализ ситуаций
- Мозговой штурм
- Интерактивное обсуждение
- Работа в малых группах
- Практическое моделирование ситуаций

Ожидаемые результаты

- **Личностные:** формирование ответственного отношения к защищённости в Интернете
- **Метапредметные:** развитие умения анализировать информационные опасности
- **Предметные:** знание основных принципов защищённого поведения в Интернете

Предварительная работа педагога

- Подготовка презентации
- Создание рабочих листов, облака слов
- Написание тестовых заданий
- Разработка технологической и интеллект-карты
- Составление кроссворда
- Поиск видеоуроков и видеороликов

Оборудование и оформление кабинета

- Компьютер с доступом в интернет
- Проектор
- Экран
- Раздаточный материал
- Рабочие листы
- Карточки с заданиями для групповой работы

Ход занятия / Ход мероприятия

Организационный момент

Здравствуйте, ребята! Рад всех видеть. Давайте проведём перекличку.

(Учитель по журналу отмечает присутствующих)

Прежде чем мы начнем наше занятие, проверьте, всё ли у вас готово к занятию. На партах должны быть: тетрадь, ручка, учебник. Всё остальное уберите в рюкзаки, чтобы ничего не отвлекало от работы.

Так, посмотрю внешний вид… Отлично, все выглядят подтянуто и опрятно, как и положено будущим защитникам Родины.

Дежурные, будьте добры, подготовьте проекционный экран – он нам сегодня понадобится для просмотра важных материалов.

Напоминаю о правилах поведения: поднимаем руку, если хотим ответить; не перебиваем говорящего; внимательно слушаем говорящего. И, конечно же, прошу всех отключить мобильные телефоны или перевести их в беззвучный режим – они нам сегодня не понадобятся.

Ребята, я вижу, что вы немного сонные после предыдущего занятия. Давайте сделаем небольшую бодрящую разминку! Встаньте, пожалуйста. Поднимите руки вверх, потянитесь как следует… Сделайте глубокий вдох… и выдох. Повторите. Повернитесь к соседу по парте и улыбнитесь друг другу. Отлично! А теперь садитесь.

Вот теперь я вижу ваши сияющие глаза и боевой настрой. Уверен, сегодняшняя наша встреча будет очень интересной и полезной для каждого из вас. Мы с вами рассмотрим важные вопросы, которые касаются каждого современного человека.

Актуализация усвоенных знаний

Дорогие девятиклассники, на прошлом занятии мы с вами говорили на тему «Современные увлечения. Их возможности и риски» . Давайте освежим в памяти ключевые моменты. Проведём небольшой блиц-опрос.

Кто может назвать основные типы молодёжных хобби? Да, Иванов, слушаем тебя… А кто дополнит ответ?

Теперь давайте подумаем – какие возможности для личностного развития дают увлечения? Петрова, поделишься своим мнением?

А теперь более серьёзный вопрос – помните, мы обсуждали риски, связанные с современными увлечениями? Кто может перечислить основные опасности? Правильно, молодцы.

Григорьев, расскажи, пожалуйста, какие коммуникативные риски могут возникнуть при общении в рамках хобби?

И последний вопрос – давайте вспомним основные стратегии безопасного взаимодействия, которые мы разбирали. Кузнецова, начни, пожалуйста, а остальные дополнят.

Отлично! Вижу, что материал прошлого занятия вы усвоили хорошо. Особенно важно то, что вы запомнили правила безопасного поведения при реализации своих любимых занятий.

А сейчас я предлагаю каждому подумать и ответить на такой вопрос: какие из современных увлечений чаще всего связаны с использованием технических устройств и интернета?

Хорошо, есть желающие поделиться своими размышлениями? … Да, совершенно верно. Практически все современные увлечения так или иначе связаны с цифровыми технологиями. И это подводит нас к теме сегодняшнего занятия.

Вступительное слово учителя

Ребята, в современном мире практически невозможно представить нашу жизнь без гаджетов, интернета и социальных сетей. Каждый день мы проводим много времени в цифровом пространстве – общаемся с друзьями, учимся, развлекаемся, ищем информацию.

Приведу пример: вы просыпаетесь утром и что первым делом берёте в руки? Правильно, телефон! Проверяете сообщения, просматриваете новости, заходите в социальные сети… А задумывались ли вы когда-нибудь, насколько безопасно ваше путешествие по цифровому миру?
Знаете, электронная среда похожа на большой город. В нём есть и прекрасные возможности, и опасные районы, и недобросовестные люди. И как в реальном городе, здесь нужно знать правила безопасного поведения.

Именно поэтому сегодня тема нашего урока: «Цифровая среда – её возможности и риски. Общие принципы безопасности в цифровой среде».

(Запишите, пожалуйста, тему в тетради.)

На этом занятии мы с вами разберём, что такое цифровая среда, какие возможности она открывает перед нами, и – что особенно важно – какие опасности могут нас подстерегать в виртуальном пространстве и как от них защититься.

> ***Цитата:***
> ***«Технологии должны служить нам, а не мы – им. И чем больше мы о них знаем, тем проще жить в мире их возможностей и угроз».***
> ***— С.Л. Мельников, 1962–2020, эксперт по безопасности, автор книг.***

Уверен, эти знания пригодятся каждому из вас, ведь все мы являемся активными пользователями Интернета. А теперь давайте начнём наше путешествие в мир электронной безопасности!

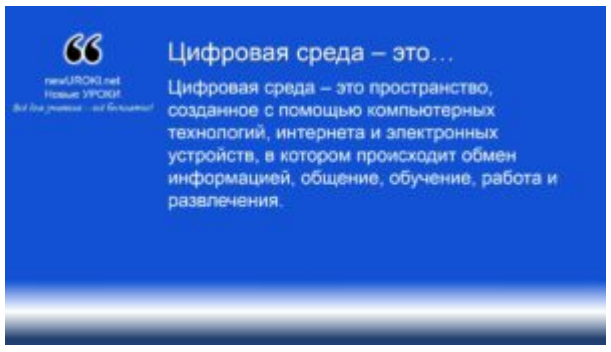
Основная часть

Иллюстративное фото / newUROKI.net

Понятие и характеристики цифровой среды

Определение

> ***Цифровая среда – это** пространство, созданное с помощью компьютерных технологий, интернета и электронных устройств, в котором происходит обмен информацией, общение, обучение, работа и развлечения.*



Определение

Она состоит из множества компонентов, среди которых можно выделить:

- Интернет – глобальная сеть, обеспечивающая доступ к информации, общению и онлайн-сервисам.
- Социальные сети – платформы, где люди общаются, обмениваются мнениями и контентом.
- Образовательные ресурсы – онлайн-курсы, видеоуроки, библиотеки.
- Электронная коммерция – интернет-магазины, платформы для продаж и покупок.
- Цифровые сервисы – банковские приложения, госуслуги, облачные хранилища.
- Виртуальная и дополненная реальность – технологии, позволяющие создать искусственные диджитал-миры.

Инфографика / newUROKI.net

Основные характеристики современной диджитал-среды

Она обладает рядом ключевых характеристик:

- **Глобальность** – интернет соединяет миллиарды людей по всему миру, предоставляя доступ к информации и взаимодействию без географических границ.
- **Доступность** – диджитал-технологии позволяют людям работать, учиться, развлекаться и общаться в любое время и в любом месте.
- **Интерактивность** – пользователи могут не только получать информацию, но и активно взаимодействовать с ней, создавая и редактируя контент.
- **Скорость обмена данными** – информация передается мгновенно, что делает эту среду удобной для работы и общения.
- **Персонализация** – алгоритмы искусственного интеллекта анализируют предпочтения пользователей и предлагают индивидуальный контент.

- **Анонимность (условная)** – в интернете человек может скрыть свою личность, но при этом оставляет цифровые следы.
- **Опасности и угрозы** – электронное пространство несет не только удобства, но и риски, такие как киберпреступность, мошенничество, утечка данных.

Роль диджитал-среды в жизни современного человека

Современный человек ежедневно взаимодействует с электронным миром.

Она затрагивает практически все сферы жизни:

- **Образование:** дистанционное обучение, онлайн-курсы, электронные учебники и тестирования.
- **Работа и бизнес:** удаленная работа, онлайн-конференции, документооборот.
- **Общение:** социальные сети, мессенджеры, видеозвонки позволяют оставаться на связи с родными и друзьями.
- **Развлечения:** онлайн-игры, стриминговые сервисы, виртуальные туры.
- **Финансовые операции:** интернет-банкинг, электронные кошельки, онлайн-покупки.
- **Медицина:** онлайн-консультации врачей, цифровые медкарты, дистанционная диагностика.
- **Государственные услуги:** электронные паспорта, записи в больницу, оплата налогов через интернет.

Таким образом, цифровая среда неотъемлемо связана с повседневной жизнью, предоставляя огромные возможности, но требуя ответственного и осознанного подхода к ее использованию.

Положительные возможности цифровой среды

Иллюстративное фото / newUROKI.net

Образовательные ресурсы и дистанционное обучение

Современные технологии значительно расширили доступ к знаниям. Онлайн-платформы, электронные учебники, видеолекции и интерактивные курсы позволяют получать образование независимо от местоположения. Дистанционное обучение дает возможность изучать любые предметы в удобном темпе, а также взаимодействовать с преподавателями и экспертами по всему миру.

Популярные образовательные сервисы включают:

- Видеоуроки и лекции (RUTUBE, Coursera, Лекторий Достоевский);
- Онлайн-курсы и тренинги (Stepik, Skillbox, GeekBrains);
- Электронные библиотеки (Национальная электронная библиотека, LitRes, Lib.Ru: Библиотека Максима Мошкова);
- Платформы для подготовки к экзаменам (Решу ЕГЭ, Фоксфорд, Учи.ру).

Инфографика / newUROKI.net

Использование таких ресурсов помогает осваивать сложные темы, готовиться к экзаменам и получать новые навыки. Особенно актуальна эта перспектива для школьников, которые могут дополнительно изучать предметы и углублять свои знания.

Коммуникационные возможности и социальные связи

Современные технологии позволяют людям легко поддерживать связь, даже находясь в разных странах. Социальные сети, видео звонки, мессенджеры и форумы дают способы для общения с друзьями, заводить новые знакомства, обмениваться опытом и участвовать в дискуссиях.

Стоит прочесть также: Современные увлечения - конспект урока

Основные форматы общения в онлайн-пространстве:

- Мессенджеры (Telegram, VK) – текстовые и голосовые сообщения, звонки;
- Социальные сети (ВКонтакте, Одноклассники) – публикации, чаты, лайвы;
- Видеосвязь (Zoom, Skype, Google Meet) – видеоконференции, онлайн-собрания;
- Форумы и чаты (Reddit, Discord, специализированные площадки) – обсуждение интересных тем.

Благодаря этому взаимодействие становится удобным, быстрым и доступным. Однако важно помнить о безопасности: не стоит делиться личной информацией с незнакомцами и доверять всему, что публикуется в интернете.

Интерактивные сервисы и их роль в повседневной жизни

Технологические платформы значительно упрощают выполнение многих бытовых задач. Благодаря им можно заказывать еду, оплачивать счета, записываться к врачу, управлять финансами, планировать поездки и даже контролировать умный дом.

Основные категории сервисов, облегчающих жизнь:

- Финансовые приложения (СберБанк Онлайн, Т-Банк, Qiwi) – управление счетами, платежи, переводы;
- Доставки товаров и еды (Яндекс.Еда, Delivery Club, Ozon, Wildberries);
- Госуслуги (портал «Госуслуги») – запись к врачу, оформление документов, оплата штрафов;
- Транспортные приложения (Яндекс Go, BlaBlaCar, общественный транспорт) – вызов такси, планирование маршрутов;
- Здоровье и спорт (Strava, MyFitnessPal, Zdorovie.ru) – контроль физической активности, консультации врачей.

Использование таких платформ делает повседневные задачи более удобными, сокращает время на рутинные дела и помогает эффективнее управлять личными ресурсами.

Профессиональное развитие в виртуальной среде

Технологии не только помогают в учебе, но и открывают новые возможности для карьеры. С развитием удаленной работы многие компании предлагают вакансии без привязки к офису, а интернет позволяет изучать новые профессии и зарабатывать деньги в онлайн-формате.

Главные направления профессионального роста в цифровом мире:

- Удаленная работа (фриланс, онлайн-работа, проекты);
- Онлайн-обучение (курсы по программированию, дизайну, маркетингу, аналитике);
- Сетевой нетворкинг (поиск работы через LinkedIn, биржи фриланса);
- Развитие персонального бренда (ведение блога, создание контента, онлайн-предпринимательство).

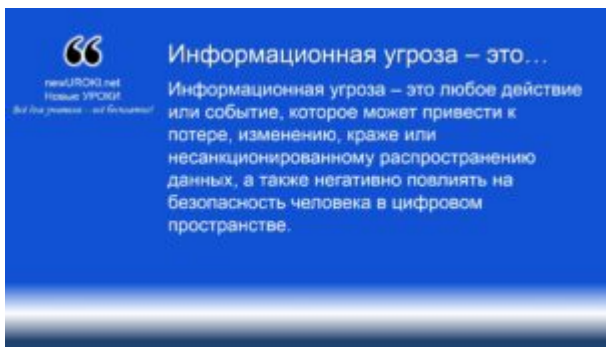
Благодаря таким возможностям люди могут работать из любой точки мира, осваивать востребованные профессии и повышать свою конкурентоспособность на рынке труда.

Технологические инструменты делают жизнь удобнее, помогают учиться, работать, общаться и развиваться. Однако наряду с преимуществами важно учитывать риски и использовать виртуальное пространство осознанно и безопасно.

Информационные и компьютерные угрозы

Иллюстративное фото / newUROKI.net

> ***Информационная угроза – это** любое действие или событие, которое может привести к потере, изменению, краже или несанкционированному распространению данных, а также негативно повлиять на безопасность человека в цифровом пространстве.*



Определение

Классификация цифровых рисков

Все потенциальные опасности, связанные с обработкой, хранением и передачей сведений, можно разделить на несколько категорий:

- **Технические проблемы** – сбои в работе оборудования, программные ошибки, повреждение файлов.
- **Зловредные программы** – вирусы, трояны, шпионские утилиты, которые нарушают работоспособность устройств.

- **Манипулятивные методы** – психологические приемы, с помощью которых мошенники обманывают пользователей.
- **Нарушение конфиденциальности** – кража персональных сведений, публикация личных сведений без согласия владельца.

Каждый из этих факторов может привести к серьезным последствиям: от потери доступа к аккаунтам до финансового ущерба и утечки важной информации.

Вредоносное программное обеспечение

Зараженные файлы и опасные приложения представляют одну из главных угроз для пользователей сети. Опасные программы могут проникнуть в систему различными способами: через скачивание неизвестных файлов, открытие подозрительных ссылок или уязвимости в программном обеспечении.

Основные виды вредоносного кода:

- **Вирусы** – программы, которые самостоятельно распространяются по системе, изменяют или удаляют файлы.
- **Черви** – вредоносные объекты, способные копировать себя и отправлять через сеть другим пользователям.
- **Трояны** – скрытые программы, маскирующиеся под полезные приложения, но выполняющие вредоносные функции.
- **Руткиты** – утилиты, которые помогают злоумышленникам получать скрытый доступ к устройству.
- **Шпионское ПО** – программы, которые незаметно собирают сведения о пользователе (логины, пароли, переписку).
- **Блокировщики** – утилиты, ограничивающие доступ к системе или файлам с целью вымогательства денег.

Инфографика / newUROKI.net

Чтобы избежать заражения, необходимо устанавливать антивирусное ПО, скачивать файлы только из надежных источников и регулярно обновлять операционную систему.

Методы социальной инженерии

Помимо вирусных программ, мошенники используют различные психологические приемы, заставляя пользователей самостоятельно передавать им личные данные. Это направление называется социальной инженерией и основано на умении манипулировать доверием человека.

Основные методы:

- **Фишинг** – отправка поддельных писем или сообщений с просьбой ввести логин и пароль.
- **Вишинг** – телефонные звонки от якобы представителей банка, полиции или службы поддержки, убеждающие назвать конфиденциальные сведения.
- **Смишинг*** – рассылка СМС-сообщений со ссылками на вредоносные сайты.
- **Претекстинг*** – обман, при котором злоумышленник создает доверительную ситуацию, например, представляясь другом или коллегой.

- **Байт-джекеринг** – создание поддельных Wi-Fi сетей, через которые можно перехватывать переписку и логины пользователей.

> ***Смишинг** — вид фишинга через SMS. Мошенники отправляют жертве SMS-сообщение, содержащее ссылку на фишинговый сайт и мотивирующее её войти на этот сайт. Википедия*
>
> ***Претекстинг (pretexting)** — это вид социальной инженерии, при котором злоумышленник использует ложную историю или предлог для получения конфиденциальной информации или доступа к защищённой системе. Пример претекстинга: злоумышленник представляется ИТ-специалистом и просит у сотрудника данные для «проверки учётной записи» или «обновления пароля». Также претекстинг может включать создание фальшивых идентификационных документов или взлом электронных учётных записей, чтобы выдать себя за другого человека и получить доступ к информации или системе. **Яндекс.Нейро***

Чтобы не стать жертвой таких манипуляций, важно проверять отправителей сообщений, не раскрывать личную информацию посторонним и использовать двухфакторную аутентификацию для защиты аккаунтов.

Нарушение конфиденциальности личных данных

Одной из самых серьезных проблем в цифровом пространстве является утечка личной информации. Это может произойти по разным причинам: взлом аккаунтов, неосторожное поведение в социальных сетях, установка небезопасных приложений.

Основные риски:

- Перехват паролей – использование слабых комбинаций или повторное применение одного и того же пароля на разных сайтах.
- Публикация личных сведений – размещение в открытом доступе фотографий, документов, номеров телефонов.
- Отсутствие защиты профилей – неправильные настройки приватности в социальных сетях.
- Сбор информации сторонними сервисами – некоторые приложения могут передавать данные пользователей рекламодателям или третьим лицам.

Чтобы снизить вероятность утечки данных, необходимо использовать сложные пароли, настраивать конфиденциальность в соцсетях, не переходить по сомнительным ссылкам и регулярно проверять, какие приложения имеют доступ к личной информации.

Опасности в цифровой среде могут принимать разные формы – от вредоносных программ до манипулятивных схем мошенников. Однако если соблюдать простые правила безопасности, можно минимизировать риск и защитить свои персональные данные.

Риски использования интернета

Иллюстративное фото / newUROKI.net

Обман в виртуальном пространстве

Злоумышленники часто используют различные схемы для получения чужих средств или данных. Например, они могут создавать поддельные сайты интернет-магазинов, где предлагают товары по слишком низким ценам. Представьте ситуацию: вы нашли крутые наушники за полцены, а после оплаты вам прислали старую проводную гарнитуру вместо современного гаджета. Это типичный пример обмана.

Психологическое давление и манипуляции

- **Кибербуллинг** – это когда кто-то систематически унижает или оскорбляет других пользователей через сообщения или комментарии. Например, группа одноклассников может начать распространять ложные слухи о человеке в социальной сети, что сильно повлияет на его психологическое состояние.
- **Груминг*** – более опасная форма воздействия, когда взрослые пытаются завоевать доверие подростков для недопустимых целей.

> ***Груминг, долговременное установление взрослым близких, доверительных отношений с ребёнком с целью завоевания доверия и последующего совращения. Используется для вовлечения несовершеннолетних в различные незаконные виды деятельности, такие как торговля детьми, детская проституция, производство детской порнографии. Википедия***

Деструктивный контент

В интернете можно найти огромное количество полезной информации, но также встречаются ресурсы, пропагандирующие насилие, экстремизм, употребление запрещенных веществ и другие опасные идеи.

- **Негативное влияние блогеров** – некоторые авторы продвигают нездоровые идеи (например, культ худобы, асоциальное поведение или опасные челленджи).
- **Группы с вредным контентом** – склоняющие подростков к опасным поступкам, вовлекать в криминальные схемы.
- **Фейки и дезинформация** – распространение ложных сведений, которые способны вводить людей в заблуждение.

Пример для учеников: Вы смотрите ролик, где блогер утверждает, что можно легко заработать деньги, просто введя данные своей банковской карты на «секретном сайте». Это пример опасной информации.

Зависимость от сети

Многие подростки проводят слишком много времени онлайн, что может привести к проблемам в реальной жизни. Например, вместо того чтобы заниматься спортом или общаться с друзьями лично, некоторые выбирают бесконечные часы в играх или просмотре видео. Это может повлиять на учебу, здоровье и отношения с близкими.

Для лучшего понимания предлагаю вам поработать с конкретными ситуациями. Каждая группа получает карточку с описанием рискованного случая:

1. Одна группа анализирует пример мошенничества (например, покупка несуществующего аккаунта в игре)
2. Другая разбирает случай кибербуллинга (например, конфликт в групповом чате)
3. Третья рассматривает встречу с деструктивным контентом (например, случайное обнаружение опасных челленджей)
4. Четвертая изучает историю зависимости (например, проблемы с успеваемостью из-за чрезмерного увлечения играми)

После анализа каждая команда представляет свои выводы и предлагает способы действий в подобной ситуации. Это поможет вам лучше понять, как распознать потенциальные опасности и научиться им противостоять.

Принципы безопасного поведения в цифровой среде

Иллюстративное фото / newUROKI.net

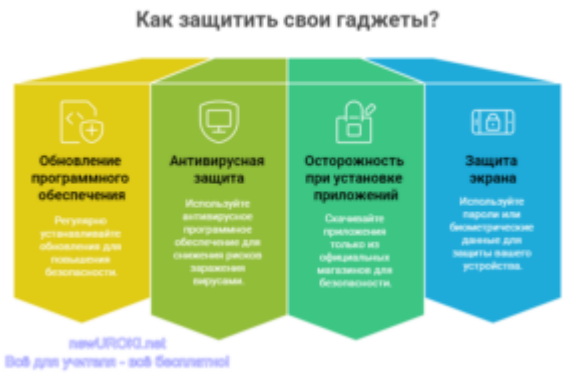
Современные технологии открывают перед человеком множество возможностей, но также требуют ответственного подхода к защите личных данных и коммуникации в виртуальном мире. Соблюдение определенных правил помогает минимизировать риски и сохранять персональную информацию в безопасности.

Защита персональных устройств

Каждый человек ежедневно использует смартфоны, ноутбуки и планшеты для работы, учебы и общения. Однако если не соблюдать базовые меры предосторожности, устройства могут стать уязвимыми для вредоносных программ и хакерских атак.

Как защитить свои гаджеты:

- **Обновление программного обеспечения** – важно регулярно устанавливать обновления для операционной системы и приложений, поскольку разработчики устраняют уязвимости, которыми могут воспользоваться злоумышленники.
- **Антивирусная защита** – использование антивирусных программ снижает риск заражения вирусами, способными украсть данные или повредить файлы.
- **Осторожность при установке приложений** – скачивать программы следует только из официальных магазинов (Google Play, App Store), чтобы избежать вредоносного ПО.
- **Защита экрана блокировкой** – использование паролей, PIN-кодов, отпечатков пальцев или Face ID предотвращает доступ посторонних к персональной информации.



Инфографика / newUROKI.net

Пример для учеников: Представьте, что ваш друг скачал бесплатную игру с неизвестного сайта, а через несколько дней его телефон начал зависать, а с банковской карты списались деньги. Это могло произойти из-за установки вредоносного приложения.

Управление личной репутацией в интернете

Любые публикации, комментарии и фото, размещенные в сети, формируют представление о человеке. Даже спустя годы неосторожные высказывания могут сыграть негативную роль, например, при устройстве на работу или поступлении в университет.

Как сохранить положительный имидж:

- Обдумывайте публикации – перед тем как выложить пост или комментарий, задайте себе вопрос: «Не пожалею ли я об этом через год?»
- Удаление компрометирующего контента – если в соцсетях есть старые фотографии или записи, которые могут вас выставить в плохом свете, лучше их удалить.
- Приватность аккаунтов – ограничьте круг лиц, которые могут видеть ваш профиль и личную информацию, настройте доступ к публикациям.
- Фильтр друзей – добавляйте в список контактов только тех, кого действительно знаете.

Пример для учеников: В одной компании кандидат не смог устроиться на работу, потому что работодатель нашел его старые посты с агрессивными комментариями. Это пример того, как виртуальная активность влияет на реальную жизнь.

Стоит прочесть также: ЧС: наводнения - конспект урока

Безопасные пароли и двухфакторная аутентификация

Пароль – это первая линия защиты учетной записи. Чем он сложнее, тем труднее злоумышленникам взломать аккаунт.

Правила создания надежных комбинаций:

- Длина – не менее 12 символов.
- Использование букв разного регистра, цифр и специальных символов.
- Исключение простых слов и дат (например, «qwerty123», «2008» – плохие пароли).
- Разные учетные записи – разные коды (не стоит использовать одну и ту же комбинацию для всех сайтов).
- Дополнительная защита – двухфакторная аутентификация (2FA). Это система, при которой вход требует не только пароля, но и кода подтверждения, отправленного на телефон или e-mail.

Пример для девятиклассников: Представьте, что ваш друг использует пароль «123456» для соцсетей и электронной почты. Однажды его аккаунт взламывают, а мошенники рассылают друзьям фальшивые просьбы о помощи с переводом денег. Если бы он использовал сложный секретный код и 2FA, этого можно было бы избежать.

Правила безопасного общения в сети

Общение в интернете кажется безобидным, но именно здесь часто случаются манипуляции, кибербуллинг и мошенничество.

Как избежать неприятностей:

- Не доверять незнакомцам – если кто-то пишет с просьбой отправить деньги, личные фото или поделиться кодом доступа, скорее всего, это обман.
- Блокировать агрессивных пользователей – если в комментариях или личных сообщениях появляется негатив, лучше не отвечать, а заблокировать отправителя.
- Осторожность с личными данными – не стоит выкладывать в открытый доступ номер телефона, адрес и другую конфиденциальную информацию.
- Остерегаться подозрительных ссылок – если даже знакомый прислал странную ссылку, лучше уточнить, действительно ли он это сделал.

Пример для школьников: Вам пишет незнакомец, представляется вашим одноклассником и просит переслать код из СМС, якобы для голосования. Скорее всего, это попытка взлома аккаунта.

Безопасность в виртуальном пространстве – это не просто набор правил, а образ жизни современного человека. Соблюдение элементарных мер предосторожности поможет защитить персональные данные, избежать неприятных ситуаций и комфортно пользоваться интернетом. Помните: чем осознаннее вы подходите к использованию онлайн-технологий, тем меньше вероятность столкнуться с проблемами!

Таблица: Способы защиты личных данных

Метод	Описание
Надежные пароли	Использование сложных комбинаций
Двухэтапная проверка	Дополнительный уровень безопасности
Антивирусное ПО	Защита от вредоносных программ
Ограничение доступа	Настройка прав для разных пользователей
Проверка источников	Использование только проверенных ресурсов

Практическая безопасность в личном цифровом пространстве

Иллюстративное фото / newUROKI.net

Управление конфиденциальностью в соцсетях

Настройки доступа к вашему профилю – это важный инструмент для контроля того, кто видит ваши данные. Например, если вы установите ограничение на просмотры фото только для друзей, случайные люди не смогут использовать ваши снимки в неподобающих целях. Важно регулярно проверять эти параметры, так как платформы часто обновляют свои функции.

Проверка достоверности информации

При получении новостей или информации из интернета всегда проверяйте источник. Представьте ситуацию: вы читаете о новом способе заработать деньги быстро и легко. Прежде чем верить этому, найдите информацию на авторитетных ресурсах или официальных сайтах. Если новость кажется слишком удивительной, скорее всего, это ложь.

Создание резервных копий

Всегда делайте бэкап важных файлов. Это может быть учебный проект, семейные фотографии или другие значимые материалы. Например, если вы работаете над курсовой работой несколько недель, внезапная поломка компьютера может все испортить. Регулярное копирование данных на внешний диск или облачное хранилище поможет избежать таких проблем.

Алгоритм действий при столкновении с угрозами

Если вы столкнулись с угрозой, нужно действовать по алгоритму:

- Прекратить взаимодействие с источником опасности
- Сменить пароли от всех аккаунтов
- Сообщить родителям или доверенному взрослому
- При необходимости обратиться в службу поддержки сервиса

Например, если вы заметили, что кто-то пытается получить доступ к вашему аккаунту, сразу измените пароль и активируйте дополнительную защиту.

Давайте выполним практическое задание «Создание безопасного профиля».

Каждый ученик должен:

- Проверить текущие настройки приватности своего аккаунта
- Найти три проверенных источника информации о последних событиях
- Создать резервную копию важных файлов
- Разработать свой план действий на случай возможной опасности

После выполнения задания мы проведем мини-конференцию, где каждый сможет поделиться результатами своей работы. Это поможет вам лучше понять, как применять полученные знания на практике и создать надежную защиту для своих данных и устройств.

Рефлексия

Теперь давайте проведём рефлексию. Важно понять, что мы не просто изучали теорию, но и пытались применить полученные знания на практике. Я предлагаю вам оценить, насколько полезным для вас был это занятие, и какие моменты вам запомнились.

Как вы думаете, что нового вы узнали сегодня о безопасности в интернете? Какие моменты были для вас особенно интересными или неожиданными? Подумайте, как эти знания могут пригодиться вам в реальной жизни. Например, какие шаги вы будете предпринимать, чтобы защитить свою личную информацию в сети?

Сейчас даю вам минуту, чтобы подумать над следующими вопросами:

- Чувствуете ли вы, что теперь будете более уверенно себя вести в интернете?
- Какие конкретные изменения вы планируете в своей онлайн-активности?
- Какие опасности, о которых мы сегодня говорили, кажутся вам наиболее актуальными?

Вы можете поделиться своими мыслями с соседями, а затем мы обсудим все вместе. Убедитесь, что каждый из вас имеет возможность выразить своё мнение.

Помимо этого, для более глубокого анализа, попробуем вспомнить, какие практические рекомендации мы выведем из сегодняшнего занятия. Например, как правильно настраивать приватность в социальных сетях или что делать, если вас пытаются обмануть в интернете. Это поможет вам чувствовать себя более уверенно и безопасно в цифровом мире.

Давайте подумайте, что ещё мы могли бы добавить к теме нашего занятия, чтобы сделать её еще более полезной и практичной.

Заключение

Учителя шутят

Сегодня мы с вами не только погрузились в захватывающий и важный мир онлайн-безопасности, но и узнали, как избежать множества подводных камней, которые могут встретиться в нашем виртуальном путешествии. Каждый из вас теперь вооружён важными знаниями, которые помогут чувствовать себя уверенно и защищённо в мире технологий.

Стоит помнить, что эти умения помогут не только избежать неприятных ситуаций, но и развить ответственность, что в будущем станет важной частью вашей жизни. Уверенность в своих силах и знаниях — это ключ, который откроет для вас новые возможности и облегчит путь к успеху.

Не забывайте, что вы — хозяева своей безопасности и своего времени. Будьте внимательны, осознавайте риски, но не бойтесь использовать все те ресурсы, которые предоставляет современная жизнь. Вы можете не только защищать себя, но и помогать окружающим, становясь примером правильного поведения в сети.

Я уверен, что вы сможете применить полученные знания и навыки не только в учебе, но и в повседневной жизни, оставаясь уверенными, ответственными и готовыми к любым вызовам.

Домашнее задание

Ученики шутят

Обязательная часть:

- Составить памятку «Моя цифровая безопасность» с основными правилами безопасного поведения в сети
- Проанализировать настройки приватности в своих социальных сетях

По желанию:

- Подготовить мини-проект «Безопасный профиль» — разработать рекомендации по защите личного аккаунта в социальной сети
- Создать инфографику по теме «Угрозы в цифровой среде и способы защиты»

Технологическая карта

Скачать бесплатно технологическую карту урока по теме: «Цифровая среда — ее возможности и риски. Общие принципы безопасности в цифровой среде»

Технологическая карта — это документ, который содержит структуру и планирование учебного занятия, включая цели, задачи, этапы, методы и формы организации деятельности учащихся, а также используемые ресурсы и оборудование.

Смотреть видео по теме

Полезные советы учителю

Скачать бесплатно 5 полезных советов для проведения урока основ безопасности и защиты Родины по теме: «Цифровая среда» в формате Ворд

Чек-лист педагога

Скачать бесплатно чек-лист для проведения урока ОБЗР по теме: «Цифровая среда» в формате Word

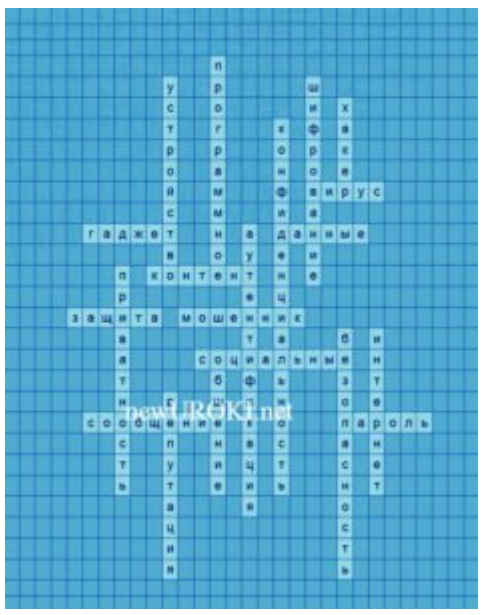
Чек-лист для учителя — это инструмент педагогической поддержки, представляющий собой структурированный перечень задач, шагов и критериев, необходимых для успешного планирования, подготовки и проведения урока или мероприятия.

Карта памяти для учеников

Скачать бесплатно карту памяти для учеников 9 класса по ОБЗР по теме: «Цифровая среда» в формате Ворд

Карта памяти ученика — это методический инструмент, который помогает учащимся структурировать и запоминать ключевую информацию по определенной теме.

Кроссворд



Кроссворд

Скачать бесплатно кроссворд на урок ОБЗР в 9 классе по теме: «Цифровая среда — ее возможности и риски. Общие принципы безопасности в цифровой среде» в формате WORD

Тесты

Какой процент современных подростков проводит более 4 часов в день за компьютером?
a) 30%
b) 55%
c) 85%
Правильный ответ: c

При создании надёжного пароля следует использовать:
a) Только строчные буквы
b) Комбинацию букв, цифр и специальных символов
c) Простые запоминающиеся слова
Правильный ответ: b

Как часто рекомендуется менять пароли от важных аккаунтов?
a) Раз в 2-3 месяца
b) Раз в год
c) Никогда не менять
Правильный ответ: a

Что делать при получении подозрительного письма?
a) Открыть все вложения
b) Переслать друзьям
c) Удалить без открытия
Правильный ответ: c

Признак фишингового сообщения:
a) Предложение срочно ввести личные данные
b) Уведомление о плановых работах
c) Письмо от знакомого адресата
Правильный ответ: a

Как защитить личные файлы на устройстве?
a) Хранить их в общем доступе
b) Создавать резервные копии
c) Удалить все данные
Правильный ответ: b

При обнаружении вредоносной программы следует:
a) Проигнорировать предупреждение
b) Запустить антивирусную проверку
c) Отключить защиту
Правильный ответ: b

Безопасное общение предполагает:
a) Отправку личных фото незнакомцам
b) Разглашение домашнего адреса
c) Сохранение конфиденциальности данных
Правильный ответ: c

Как часто следует обновлять защитные программы?
a) Автоматически при появлении обновлений
b) Раз в год
c) Никогда
Правильный ответ: a

При столкновении с преследованием необходимо:

a) Игнорировать проблему

b) Сообщить взрослым и заблокировать агрессора

c) Ответить тем же

Правильный ответ: b

Интересные факты для занятия

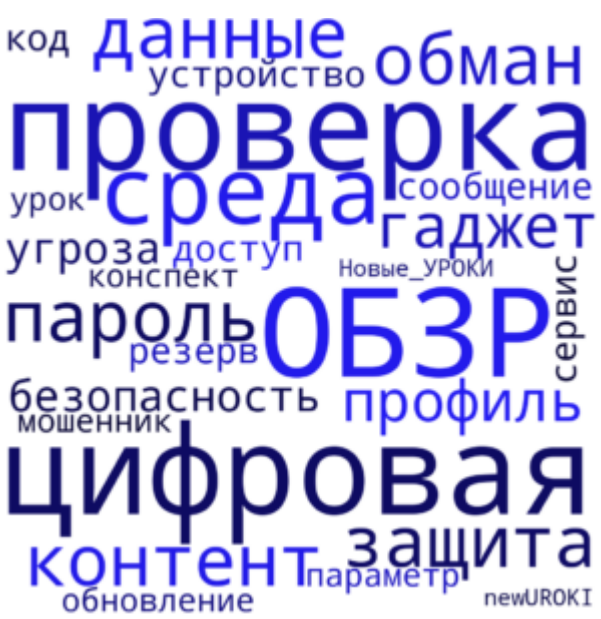
1. **Интересный факт 1:**
   В 2023 году средний подросток тратит на смартфон больше времени, чем на сон — около 9 часов ежедневно! При этом мозг вырабатывает такое же количество дофамина (гормона удовольствия), как при употреблении шоколада или катании на американских горках.
2. **Интересный факт 2:**
   Самый распространённый пароль в мире — «123456». Его используют более 23 миллионов человек! Профессиональному взломщику требуется менее секунды, чтобы подобрать такой пароль. А вот пароль из 12 символов, содержащий буквы, цифры и специальные знаки, придётся взламывать около 34 тысяч лет.
3. **Интересный факт 3:**
   В современных играх и приложениях используются специальные психологические приёмы для удержания внимания: яркие цвета, приятные звуки, система наград и достижений. Эти же техники применяются при создании игровых автоматов в казино! Именно поэтому так сложно оторваться от экрана, даже когда пора делать домашнее задание.

Интеллект-карта

Ментальная карта (интеллект-карта, mind map)

Ментальная карта (интеллект-карта, mind map) — это графический способ структурирования информации, где основная тема находится в центре, а связанные идеи и концепции отходят от неё в виде ветвей. Это помогает лучше понять и запомнить материал.

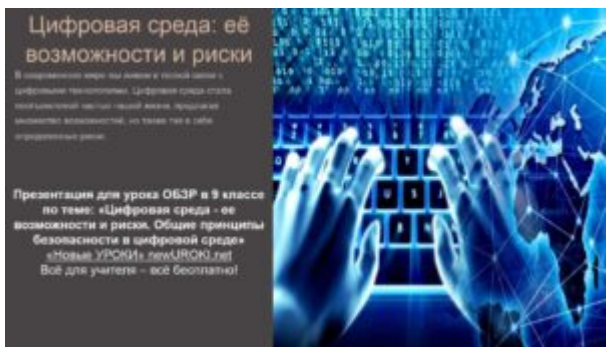
Облако слов



Облако слов

Облако слов — удобный инструмент на занятии: помогает активизировать знания, подсказывает, служит наглядным материалом и опорой для учащихся разных возрастов и предметов.

Презентация



Презентация

Скачать бесплатно презентацию на урок ОБЗР в 9 классе по теме: «Цифровая среда — ее возможности и риски. Общие принципы безопасности в цифровой среде» в формате PowerPoint

БОНУС: Рабочий лист

Скачать бесплатно рабочий лист по ОБЗР по теме: «Цифровая среда — ее возможности и риски. Общие принципы безопасности в цифровой среде» в формате ВОРД

Рабочий лист – это образовательный инструмент, представляющий собой специально подготовленный комплект заданий, упражнений или вопросов, который используется на занятии для активизации познавательной деятельности учащихся.

Список источников и использованной литературы

1. Смирнов А.В., «Безопасность коммуникаций в современном мире». Издательство «Сириус», Санкт-Петербург, 2005. 215 страниц.
2. Петрова Л.М., Кузнецов Д.А., «Защита данных и методы их сохранности». Издательство «Техносфера», Новосибирск, 2004. 192 страницы.
3. Волков Б.С., «Основы защиты персональных устройств». Издательство «Образовательные технологии», Екатеринбург, 2002. 176 страниц.
4. Морозова Т.Р., «Практические аспекты безопасности в новой реальности». Издательство «Информационные системы», Самара, 2006. 234 страницы.
5. Григорьев С.В., Романов Е.Л., «Методы противодействия угрозам в современных технологиях». Издательство «Высшая школа», Москва, 2003. 250 страниц.

0 НРАВИТСЯ 0 НЕ НРАВИТСЯ

50% Нравится Или 50% Не нравится

Скачали? Сделайте добро в один клик! Поделитесь образованием с друзьями!

Расскажите о нас!

Слова ассоциации (тезаурус) к уроку: устройство, пароль, репутация, данные, мошенник, вирус, хакер, общение, гаджет, контент, шифрование.

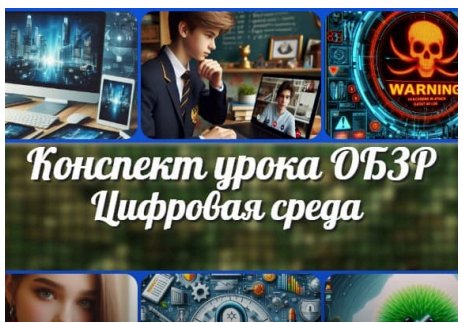
Защита прав в цифровом пространстве — конспект урока »

Автор Глеб Беломедведев

Глеб Беломедведев - постоянный автор и эксперт newUROKI.net, чья биография олицетворяет трудолюбие, настойчивость в достижении целей и экспертность. Он обладает высшим образованием и имеет более 5 лет опыта преподавания в школе. В течение последних 18 лет он также успешно работает в ИТ-секторе. Глеб владеет уникальными навыками написания авторских конспектов уроков, составления сценариев школьных праздников, разработки мероприятий и создания классных часов в школе. Его талант и энтузиазм делают его неотъемлемой частью команды и надежным источником вдохновения для других.

ПОХОЖИЕ УРОКИ

ИНТЕРЕСНЫЕ КОНСПЕКТЫ УРОКОВ



Новые УРОКИ

Новый сайт от проекта UROKI.NET. Конспекты уроков, классные часы, сценарии школьных праздников. Всё для учителя - всё бесплатно!

Добро пожаловать на сайт "Новые уроки" - newUROKI.net, специально созданный для вас, уважаемые учителя, преподаватели, классные руководители, завучи и директора школ! Наш лозунг "Всё для учителя - всё бесплатно!" остается неизменным почти 20 лет! Добавляйте в закладки наш сайт и получите доступ к методической библиотеке конспектов уроков, классных часов, сценариев школьных праздников, разработок, планирования по ФГОС, технологических карт и презентаций. Вместе мы сделаем вашу работу еще более интересной и успешной! Дата открытия: 13.06.2023