Новые УРОКИ

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

9 КЛАСС ОБЗР

Поведение в цифровой среде — конспект урока

Автор Глеб Беломедведев

ФЕВ 6, 2025 18 фото Время прочтения: 39 минут(ы)

Просмотров: 5

#безопасность, #видео, #данные, #защита, #интеллект-карта, #интересные факты, #Интернет, #карта памяти, #критическое, #кроссворд, #личность, #манипуляция, #ментальная карта, #метод, #мышление, #облако слов, #поведение, #полезные советы, #правила, #презентация, #признаки, #рабочий лист, #среда, #таблица, #тесты, #технологическая карта, #цифровая, #чек-лист

Содержание [Скрыть]

Поиск

Поиск

ИНТЕРЕСНОЕ

КОНСПЕКТЫ УРОКОВ

Правила безопасного поведения в цифровой среде — конспект урока ОБЗР (Основы безопасности и защиты Родины)

Вступление

> ***В эпоху стремительной цифровизации каждый подросток ежедневно сталкивается с виртуальными угрозами, даже не подозревая об этом. Представьте: обычный день, привычная переписка в мессенджере – и вдруг ваш ученик становится мишенью злоумышленников. Как защитить детей в постоянно меняющемся цифровом мире? В этом конспекте вы найдете не только актуальные методики обучения кибербезопасности, но и полный комплект материалов: технологическую карту, презентацию, интерактивные тесты, рабочие листы и кроссворд для закрепления материала.***

Выберите похожие названия

- Методическая разработка: «Цифровая безопасность в современном мире»
- Интегрированное занятие: «Защита от киберугроз в повседневной жизни»
- Практикум: «Информационная гигиена и противодействие манипуляциям в сети»
- Открытый урок: «Безопасное поведение в виртуальном пространстве»

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

Интерактивное занятие с использованием кейс-технологий

Цель

- Формирование у обучающихся навыков безопасного поведения в цифровой среде и умения противодействовать информационным угрозам

Задачи

- **Обучающая:** Сформировать представление о правилах безопасного поведения в цифровой среде, методах противодействия кибербуллингу и манипуляциям
- **Развивающая:** Развить критическое мышление и навыки анализа информационных угроз
- **Воспитательная:** Воспитать ответственное отношение к личной информационной безопасности

Универсальные учебные действия (УУД)

- **Личностные УУД:** Формирование ответственного отношения к собственной информационной безопасности
- **Регулятивные УУД:** Умение оценивать риски и принимать решения в нестандартных ситуациях
- **Познавательные УУД:** Развитие навыков анализа информации и выявления потенциальных угроз
- **Коммуникативные УУД:** Развитие умения взаимодействовать в цифровой среде с соблюдением норм безопасности
- **Метапредметные УУД:** Формирование целостного представления о безопасном поведении в цифровом пространстве

Методические приёмы, педагогические методы, технологии обучения

Кейс-метод

Анализ конкретных ситуаций

Ролевое моделирование

Интерактивный диалог

Мозговой штурм

Проблемное обучение

Работа в малых группах

Ожидаемые результаты

- **Личностные:** Формирование ответственного отношения к собственной безопасности в цифровой среде, развитие критического мышления при работе с информацией
- **Метапредметные:** Умение анализировать информационные угрозы, способность принимать обоснованные решения в условиях информационных рисков
- **Предметные:** Овладение навыками противодействия кибербуллингу и манипуляциям, знание алгоритмов действий в кризисных ситуациях

Предварительная работа педагога

- Подготовка презентации
- Разработка кейсов с примерами реальных ситуаций
- Создание рабочих листов для практической работы
- Написание тестовых заданий
- Составление кроссворда, технологической и интеллект-карты
- Поиск видеоуроков и видеоматериалов

Оборудование и оформление кабинета

- Компьютер с доступом в интернет
- Мультимедийный проектор
- Экран
- Раздаточный материал

- Плакаты
- Рабочие листы для практических заданий
- Памятки по кибербезопасности

Ход занятия / Ход мероприятия

Организационный момент

Здравствуйте, ребята! Прошу всех занять свои места.

(Проверка присутствующих)

Староста, доложите об отсутствующих.

(Проверка готовности к уроку)

Проверьте, все ли у вас готово к занятию — на столе должны лежать тетрадь, ручка, учебник. Уберите все лишние предметы.

(Обращение к дежурным)

Дежурные, прошу подготовить проекционный экран для работы. Проверьте, хорошо ли его видно со всех учебных мест.

(Проверка внешнего вида)

Обратите внимание на свой внешний вид — поправьте, пожалуйста, школьную форму, если это необходимо.

(Правила поведения и организационные моменты)

Напоминаю о правилах поведения:

- Поднимаем руку, если хотим ответить или задать вопрос
- Не перебиваем отвечающего
- Внимательно слушаем говорящего
- Записи в тетради ведем аккуратно

И особая просьба — переведите, пожалуйста, ваши мобильные телефоны в беззвучный режим и уберите их в сумки. Они нам сегодня не понадобятся.

(Создание позитивного настроя)

Я вижу, что сегодня вы все собранны и готовы к работе. Это очень радует! Уверен, что наше занятие будет интересным и полезным. Каждый из вас сможет узнать что-то новое и важное для себя.

Перед тем как мы начнем, давайте улыбнемся друг другу — ведь хорошее настроение помогает лучше усваивать новые знания. Я вижу, что вы полны энергии и готовы к продуктивной работе. Это именно то, что нам нужно для сегодняшнего занятия!

Актуализация усвоенных знаний

Ребята, на прошлом занятии мы с вами изучали важную тему: «Деструктивные течения в интернете, их признаки, опасности» . Давайте освежим в памяти ключевые моменты, которые помогут нам лучше усвоить сегодняшний материал.

Предлагаю вам поразмышлять над несколькими вопросами:

Вспомните, пожалуйста, что такое деструктивные течения в интернете? Кто может привести конкретный пример такого течения?

(Ожидает ответов учащихся)

Отлично. А теперь давайте подумаем – какие признаки могут указывать на то, что интернет-сообщество является разрушительным? По каким «маячкам» мы можем это определить?

(Выслушивает ответы)

Очень хорошо. Особенно важно, что вы упомянули…

(обращается к конкретному ответу ученика)

Действительно, деструктивные сообщества часто маскируются под безобидные группы по интересам.

Следующий важный момент – какие действия в интернет-пространстве считаются противоправными? И главное – какие последствия могут наступить за участие в опасных интернет-сообществах?

(Слушает ответы девятиклассников)

Да, совершенно верно. Хочу особенно подчеркнуть, что незнание закона не освобождает от ответственности. Даже если человек случайно стал участником такого сообщества, это может иметь серьезные последствия.

И последний вопрос для повторения: какую роль играют семья и общество в защите подростков от вовлечения в деструктивные течения? Приведите примеры из жизни, как родители и учителя могут помочь в этом вопросе?

(После высказываний учеников)

Прекрасно! Я вижу, что материал прошлого занятия вы усвоили хорошо. Эти знания станут надежным фундаментом для понимания нашей новой темы. Ведь сегодня мы будем говорить о том, как эти знания применить на практике в повседневной жизни.

Особенно хочу отметить ответы…

(называет 2-3 фамилии активно отвечавших учеников)

Ваши примеры были очень точными и показательными. Это демонстрирует, что вы не просто запомнили материал, но и глубоко его осмыслили.

Вступительное слово учителя

Ребята, каждый день мы с вами погружаемся в цифровой мир: общаемся в социальных сетях, обмениваемся сообщениями, ищем информацию в интернете. Этот мир открывает перед нами огромные возможности, но вместе с тем таит в себе серьезные опасности.

Представьте себе ситуацию: вы получаете сообщение от незнакомого человека, который предлагает участвовать в увлекательном онлайн-конкурсе с денежным призом. Заманчиво, не правда ли? Но как определить, реальное это предложение или за ним скрывается злоумышленник?

Или другой пример: вы случайно переходите по ссылке, и вдруг появляется окно с требованием перевести деньги, иначе ваши личные данные будут опубликованы. Что делать в такой ситуации? Как защитить себя от подобных угроз?

Именно поэтому тема нашего сегодняшнего урока – «Правила безопасного поведения в цифровой среде».

Мы с вами разберем основные виды угроз, с которыми может столкнуться каждый пользователь интернета, научимся распознавать опасные ситуации и, самое главное, узнаем, как действовать, чтобы защитить себя и своих близких.

Это занятие – не просто теория. Это жизненно важные навыки, которые пригодятся вам каждый день. Ведь в современном мире интернет-грамотность так же важна, как умение читать и писать. И наша задача – научиться быть грамотными и осторожными пользователями электронного пространства, не теряя при этом всех тех возможностей, которые оно нам предоставляет.

> ***Цитата:***
> ***«Осторожность в словах и действиях — это не признак слабости, а проявление силы разума.»***
> ***— Р.К. Сиваков, 1970–2021, российский психолог, эксперт по безопасности.***

Готовы погрузиться в мир цифровой безопасности? Тогда начнем наше путешествие!

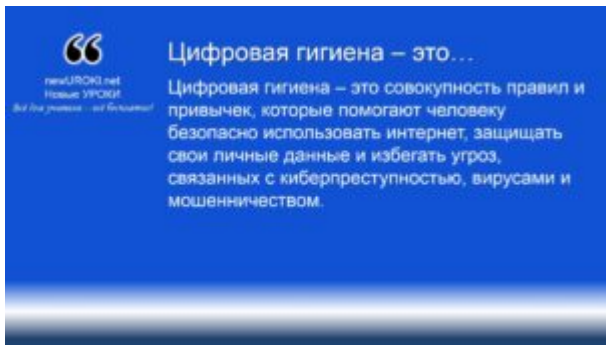
Основная часть

Иллюстративное фото / newUROKI.net

Основные принципы безопасного поведения в цифровой среде

Цифровая гигиена как основа безопасности в сети Интернет

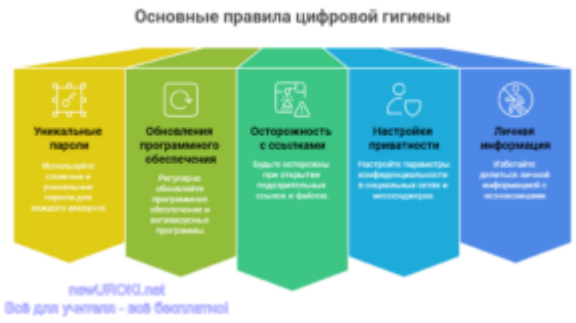
> ***Цифровая гигиена – это** совокупность правил и привычек, которые помогают человеку безопасно использовать интернет, защищать свои личные данные и избегать угроз, связанных с киберпреступностью, вирусами и мошенничеством.*



Определение

Основные правила цифровой гигиены включают:

- Использование сложных и уникальных паролей для каждого аккаунта.
- Регулярное обновление программного обеспечения и антивирусных программ.
- Осторожность при открытии подозрительных ссылок и файлов.
- Настройку приватности в социальных сетях и мессенджерах.
- Избегание передачи личной информации незнакомцам.



Инфографика / newUROKI.net

Критическое мышление при работе с информацией

В электронном пространстве огромное количество материалов, но не все они являются достоверными и безопасными. Критическое мышление – это способность анализировать новости, проверять их источник, выявлять возможные манипуляции и фейки.

Основные принципы критического мышления в интернете:

- Проверяйте источник: доверяйте только проверенным и официальным сайтам.
- Анализируйте контент: не все новости и посты в соцсетях соответствуют действительности.
- Избегайте эмоциональных решений: не поддавайтесь на провокационные заголовки и сенсационные заявления.
- Сравнивайте новости из разных источников: достоверные всегда подтверждаются несколькими независимыми источниками.
- Не распространяйте непроверенные сведения: это может нанести вред другим людям.

Инфографика / newUROKI.net

Принципы защиты личных данных и приватности

В интернете множество угроз, связанных с утечкой персональной информации. Сведения, которые мы публикуем или передаём в сети, могут быть использованы злоумышленниками в корыстных целях.

Как защитить личные данные?

- Используйте двухфакторную аутентификацию (2FA) для защиты аккаунтов.
- Ограничивайте публикацию личных сведений (адрес, номер телефона, паспортные реквизиты).
- Будьте внимательны при регистрации на сайтах – указывайте минимально необходимую информацию.
- Настройте конфиденциальность в социальных сетях – закройте профили от посторонних.
- Не используйте публичные Wi-Fi сети без VPN, так как сведения могут быть перехвачены.
- Удаляйте старые аккаунты и ненужные приложения, которые могут хранить ваши данные.

Соблюдение этих принципов поможет избежать кибератак, мошенничества и утечек данных, обеспечив безопасное пребывание в цифровом пространстве.

Таблица: Методы защиты и их описание

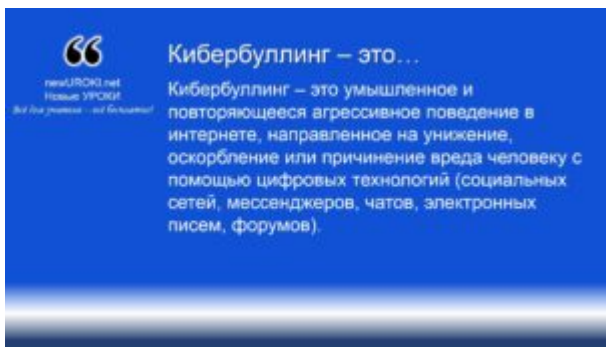
Метод защиты	Описание
Пароль	Уникальный код, предотвращающий несанкционированный доступ
Шифрование	Преобразование информации в код, понятный только получателю
Антивирус	Программа для выявления и устранения вредоносных программ
Двухфакторная проверка	Дополнительный уровень защиты при входе
Обновление системы	Установка актуальных версий программ для повышения безопасности

Кибербуллинг как форма агрессии в цифровом пространстве

Иллюстративное фото / newUROKI.net

Определение и признаки

> ***Кибербуллинг – это** умышленное и повторяющееся агрессивное поведение в интернете, направленное на унижение, оскорбление или причинение вреда человеку с помощью цифровых технологий (социальных сетей, мессенджеров, чатов, электронных писем, форумов).*



Определение

> ***Интернет-травля, или кибертравля** — намеренные оскорбления, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени. Часть киберкультуры. [Википедия]*

Признаки:

- Оскорбления, угрозы, насмешки, распространение ложной информации о человеке.
- Досаждающие сообщения, назойливые звонки или преследование в социальных сетях.
- Взлом или кража личных данных, использование их в целях шантажа.
- Публикация фото или видео без разрешения с целью унижения.
- Исключение человека из онлайн-групп с целью изоляции.

Способы противодействия кибербуллингу

Кибербуллинг может нанести серьезный психологический вред, поэтому важно знать, как ему противостоять.

Основные способы борьбы с кибербуллингом:

- Игнорирование провокаций. Не отвечайте на агрессивные сообщения, так как обидчики добиваются именно реакции.
- Блокировка агрессора. Используйте функции «Чёрный список» и «Жалоба» на платформе, где происходит буллинг.
- Сохранение доказательств. Делайте скриншоты оскорбительных сообщений или угроз, чтобы в случае необходимости обратиться за помощью.
- Сообщение взрослым. Обратитесь к родителям, учителям или школьному психологу – они помогут разобраться с ситуацией.
- Настройка конфиденциальности. Закрывайте доступ к личным данным, избегайте публикации слишком личной информации в соцсетях.
- Развитие эмоциональной устойчивости. Не позволяйте негативным комментариям влиять на вашу самооценку.

Инфографика / newUROKI.net

Алгоритм действий при столкновении с травлей в сети

Если вы стали жертвой травли, действуйте по следующему алгоритму:

- Не реагируйте эмоционально. Агрессоры питаются чужими эмоциями – не дайте им этого.
- Сделайте скриншоты угроз и оскорблений. Это поможет при разборе ситуации с администрацией соцсети, родителями или правоохранительными органами.
- Заблокируйте обидчика. Воспользуйтесь функцией блокировки или ограничьте доступ к своему профилю.
- Сообщите о ситуации взрослым. Родители, классный руководитель или школьный психолог помогут разобраться в проблеме.
- Обратитесь в техническую поддержку социальной сети. Администрация может удалить аккаунт нарушителя или ограничить его возможности.
- Если угрозы серьезные, обратитесь в полицию. Травля в некоторых случаях подпадает под статьи уголовного кодекса (например, если вам угрожают физической расправой).

- Поддерживайте друзей, если они стали жертвами интернет-травли. Иногда человеку просто нужна поддержка, чтобы справиться с проблемой.

> **Стоит прочесть также:** Безопасность пешехода - конспект урока

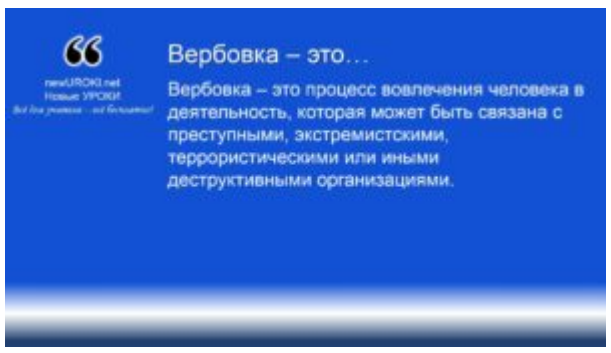
Кибербуллинг – серьезная проблема современного общества, и только осведомленность, ответственность и поддержка друг друга помогут сделать цифровую среду более безопасной для всех.

Методы вербовки через социальные сети и мессенджеры

Иллюстративное фото / newUROKI.net

Распознавание признаков вербовочной деятельности

> ***Вербовка – это** процесс вовлечения человека в деятельность, которая может быть связана с преступными, экстремистскими, террористическими или иными деструктивными организациями.*



Определение

В современном мире интернет и социальные сети стали одними из главных инструментов вербовки, поскольку они позволяют злоумышленникам оставаться анонимными и манипулировать людьми дистанционно.

Основные признаки вербовочной деятельности:

- **Неожиданное появление «доброжелателя» в сети.** Манипулятор может представляться наставником, другом, единомышленником или человеком, предлагающим интересные возможности (работу, обучение, поддержку).
- **Обещания легкого заработка или привилегий.** Часто используют заманчивые предложения: «Работа в интернете без вложений», «Секретный способ заработка» и т. д.
- **Попытки вызвать доверие.** Вербовщик изучает профиль жертвы, ее интересы, круг общения, чтобы выстроить диалог так, чтобы он казался естественным и доверительным.
- **Постепенное изменение тем общения.** Сначала разговор идет на нейтральные темы, затем – переход к более личным вопросам, обсуждению недовольства жизнью, проблемами, поиску врагов.

- **Попытки изолировать от окружения.** Он может убеждать, что родители или друзья не понимают, что жертва особенная и ей нужны «новые» люди в жизни.
- **Предложение перейти на закрытые мессенджеры.** Манипуляторы часто предлагают сменить платформу общения на более анонимную (Telegram, Signal, Tox), чтобы скрыть переписку.
- **Запрос персональных данных.** Если кто-то в сети требует персональную информацию, паспортные данные, фото с документами – это явный признак мошеннических или вербовочных действий.

Тактики манипуляции, используемые вербовщиками

Вербовщики используют психологические приемы, которые позволяют им незаметно влиять на жертву и заставлять ее выполнять нужные действия.

Основные тактики манипуляции:

- **Создание чувства исключительности.** Вербовщик внушает потерпевшей, что она особенная, умная, сильная, что именно ей предстоит изменить мир.
- **Использование страха и давления.** Могут запугивать вымышленными опасностями, говорить, что жертва в опасности и только они могут помочь.
- **Подмена ценностей.** Внедряют новые убеждения, формируют «врага», настраивают против государства, семьи, общества.
- **Игра на эмоциях.** Используют жалость, дружбу, любовь, создают эмоциональную зависимость.
- **Техники гипноза и НЛП (нейролингвистического программирования).** Использование повторяющихся слов, формул, скрытых команд, которые постепенно программируют жертву на нужные действия.
- **Постепенное вовлечение.** Манипуляторы не сразу требуют действий, а начинают с простых заданий: посмотреть видео, оставить комментарий, подписаться на закрытую группу.

Психологические приемы защиты от манипуляций

Для того чтобы не попасть под влияние вербовщиков, важно уметь противостоять их методам и знать, как себя защитить.

Основные способы защиты:

- Развитие критического мышления. Если предложение кажется слишком заманчивым или подозрительным – нужно проанализировать его и проверить информацию из независимых источников.
- Контроль личных данных. Не стоит делиться в сети информацией о себе, своих планах, местонахождении, личных документах.
- Бдительность в общении с незнакомцами. Если кто-то в интернете активно интересуется личной жизнью, финансовым положением, политическими взглядами – это повод насторожиться.
- Фильтрация контента. Следует избегать просмотра и распространения сомнительных материалов, которые могут содержать экстремистские идеи или пропаганду.
- Поддержка связи с семьей и друзьями. Преступники пытаются изолировать свой объект, поэтому важно доверять близким и не скрывать от них свои переживания.
- Игнорирование и блокировка подозрительных личностей. При малейшем подозрении на манипуляцию лучше прекратить общение и заблокировать пользователя.
- Сообщение взрослым. Если появились тревожные подозрения – лучше обсудить ситуацию с родителями, учителями или психологом.
- Обращение в правоохранительные органы. Если вам угрожают, принуждают к каким-либо действиям или требуют личные данные – это повод обратиться за помощью в полицию или Роскомнадзор.

Знание методов вербовки и умение защищаться от манипуляций – важный навык для безопасного поведения в цифровой среде. Важно помнить, что в интернете каждый может стать объектом влияния, но осведомленность и критическое мышление помогут избежать попадания в ловушку злоумышленников.

Практикум по информационной безопасности

Иллюстративное фото / newUROKI.net

Анализ реальных случаев кибербуллинга

Чтобы лучше понять, как это происходит и какие последствия может иметь, девятиклассникам предлагается рассмотреть реальные примеры подобных ситуаций.

Один из типичных случаев – создание фейковой страницы в социальной сети от имени жертвы. Представьте, что одноклассник, которому кто-то завидует или которого кто-то недолюбливает, становится объектом травли. Недоброжелатели создают поддельную страницу с его фотографиями, но подписывают оскорбительными словами или выкладывают ложную информацию о нем. Другие ученики начинают верить этим публикациям, распространять их, писать обидные комментарии. В результате жертва чувствует себя униженной, боится выходить в интернет и может даже столкнуться с депрессией.

Другой случай – групповая травля в чатах. Например, в классе создают закрытый чат, где обсуждают одного из учеников, насмехаются над ним, придумывают прозвища, делятся его неудачными фотографиями. Иногда такие чаты создаются специально для того, чтобы довести человека до слез или даже спровоцировать его удалить свои аккаунты в соцсетях. Это может привести к серьезным психологическим проблемам, ухудшению учебы и даже отказу от посещения школы.

Анализ таких случаев помогает понять, насколько кибербуллинг опасен и почему нельзя участвовать в подобных действиях, даже если это кажется шуткой. Также важно осознавать, что пострадавшим может стать любой человек, и необходимо знать, как себя защитить.

Разбор типичных схем вербовки в сети

Вербовка через интернет происходит постепенно, и далеко не всегда жертва сразу понимает, что ее вовлекают в опасную деятельность. Для того чтобы школьники научились распознавать такие угрозы, разберем несколько реальных примеров.

Одна из распространенных схем – предложение легкого заработка. Например, подростку пишут в соцсетях и предлагают удаленную работу, где не требуется никаких навыков: «Просто выполняй небольшие задания, и ты будешь получать деньги». На первом этапе поручения действительно простые – оставить комментарий, поставить лайк, поделиться публикацией. Однако затем задания становятся сложнее: подписаться на подозрительную

группу, зарегистрироваться на сомнительном сайте, отправить кому-то личные данные. На финальном этапе подростка могут даже попросить перевести деньги или участвовать в незаконных действиях.

Еще один пример – так называемая «романтическая» вербовка. Представьте, что 15-летняя девушка знакомится в интернете с парнем, который кажется ей интересным, заботливым, внимательным. Он говорит комплименты, обсуждает с ней мечты и цели, поддерживает в сложные моменты. Спустя некоторое время он начинает говорить, что они должны доверять друг другу, а значит, девушка должна рассказать ему личные секреты или отправить фото, которые не показывала никому. Если девушка это сделает, в дальнейшем ее могут шантажировать, требуя денег или принуждая к каким-то действиям.

Третья схема – манипуляция через идеологию. Человека убеждают, что он живет неправильно, что его окружают «плохие» люди, что у него должен быть «другой» путь. Постепенно его отдаляют от семьи и друзей, а потом предлагают присоединиться к закрытому сообществу, где якобы все понимают друг друга и поддерживают. На этом этапе человеку могут предложить выполнить какие-то поручения, которые сначала кажутся безобидными, но потом становятся все опаснее.

Разбирая такие случаи, школьники учатся распознавать вербовку и понимать, какие приемы используют злоумышленники. Главный вывод, который должны сделать школьники: никогда нельзя доверять незнакомцам в глобальной сети, особенно если они что-то предлагают, требуют или обещают.

Отработка навыков безопасной коммуникации

Знать теорию – это важно, но для защиты в интернете нужно уметь применять знания на практике. В этом разделе ученики выполняют упражнения, которые помогают им научиться безопасному общению в цифровой среде.

Первое задание – анализ подозрительных сообщений. Ученикам раздаются распечатанные диалоги, в которых есть признаки манипуляций, попыток вербовки или кибербуллинга. Они должны определить, какие моменты в этих диалогах настораживают, и предложить правильные способы реагирования. Например, если незнакомец спрашивает личные данные или пытается вынудить к чему-то, важно не отвечать, заблокировать собеседника и рассказать взрослым.

Второе задание – моделирование ситуации. Школьники по парам разыгрывают сценки: один играет роль злоумышленника, второй – потенциальной жертвы. Задача второго – вовремя распознать угрозу и правильно ответить. Это помогает научиться говорить «нет», не поддаваться на манипуляции и действовать уверенно.

Третье задание – работа с настройками приватности. Учащиеся заходят в свои соцсети и проверяют, насколько безопасны их аккаунты. Настраивают конфиденциальность, ограничивают доступ к личным данным, удаляют подозрительных людей из списка друзей. Это позволяет им лучше контролировать свою безопасность в интернете.

В ходе практикума школьники не только узнают о цифровых угрозах, но и получают практические навыки защиты, которые помогут им безопасно общаться в сети и не становиться жертвой злоумышленников.

Технические аспекты цифровой безопасности

Иллюстративное фото / newUROKI.net

Настройки приватности в социальных сетях

Настройки приватности — это инструменты, которые позволяют ограничить круг людей, имеющих доступ к личной информации в социальных сетях. Многие пользователи оставляют свои страницы открытыми, не осознавая, что их фотографии, переписки и публикации могут увидеть незнакомцы. Это опасно, потому что злоумышленники могут использовать личные данные в своих целях. Например, если подросток публикует информацию о своем распорядке дня или местах, которые он посещает, кто-то может начать за ним следить или даже попытаться встретиться с ним в реальной жизни.

Чтобы защитить свою страницу, нужно правильно настроить конфиденциальность. В большинстве соцсетей можно скрыть личные данные от посторонних. Например, во «ВКонтакте» можно сделать страницу закрытой, чтобы ее могли просматривать только друзья. Также можно ограничить круг лиц, которым доступны личные фотографии, истории и комментарии. Кроме того, следует отключить возможность отправки сообщений от незнакомцев. Многие школьники сталкивались с ситуацией, когда им писали подозрительные люди с предложением «подработки» или с просьбой о помощи. Если вовремя ограничить доступ, можно избежать неприятных ситуаций.

Еще один важный момент – контроль за тем, какие приложения имеют подключение к аккаунту. Часто люди привязывают свои профили к различным онлайн-играм или сервисам, не задумываясь о последствиях. Эти приложения могут собирать личные данные и даже передавать их третьим лицам. Поэтому рекомендуется регулярно проверять список приложений, имеющих подключение к аккаунту, и удалять ненужные.

Защита аккаунтов от взлома

Взлом аккаунта – одна из самых распространенных проблем среди пользователей соцсетей. Если злоумышленник получает доступ к профилю, он может отправлять от имени владельца мошеннические сообщения, менять пароль или даже удалить аккаунт. Чаще всего взлом происходит из-за слабых паролей, фишинговых атак или использования одного и того же секретного кода на разных сайтах.

Первый шаг к защите аккаунта – надежный пароль. Многие подростки используют в качестве кода подключения простые комбинации вроде «123456» или «qwerty», а также свои имена или даты рождения. Такие коды легко подобрать даже без специальных программ. Безопасный код доступа должен содержать не менее 12 символов, включая буквы разного регистра, цифры и специальные символы. Например, «8Tg#2Km&94» будет гораздо сложнее взломать, чем «максим2009».

Второй важный шаг – двухфакторная аутентификация (2FA). Это дополнительная защита, которая требует не только пароля, но и временного кода, отправляемого на телефон или email. Например, если злоумышленник узнает пароль, он все равно не сможет войти в

аккаунт без подтверждающего кода. Многие сервисы, включая Яндекс и «ВКонтакте», предлагают такую функцию, и ее обязательно нужно включить.

Еще одна распространенная угроза – фишинг. Это способ мошенничества, при котором жертву заманивают на поддельный сайт, где она сама вводит свой логин и пароль. Например, школьник получает сообщение, что его страница якобы заблокирована, и для восстановления доступа нужно перейти по ссылке. Если он перейдет и введет свои данные, они попадут в руки злоумышленников. Чтобы защититься, важно проверять адреса сайтов и не вводить коды на подозрительных страницах.

Безопасное использование публичных сетей

Публичные Wi-Fi, которые есть в кафе, школах, торговых центрах и транспорте, способны представлять угрозу безопасности. Многие люди подключаются к таким точкам, чтобы сэкономить мобильный интернет, но не задумываются о рисках. Злоумышленники могут создать поддельную точку доступа с похожим названием, например, «Free Wi-Fi», и перехватывать данные, которые вводят пользователи.

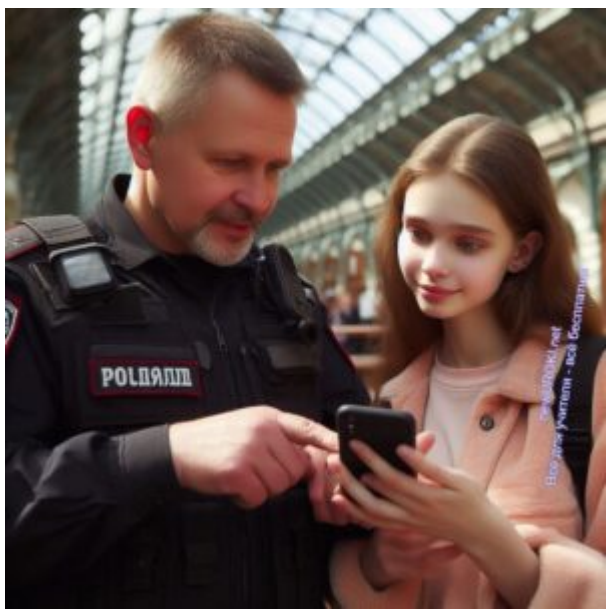
Стоит прочесть также: Психологическое воздействие - конспект урока

Например, представьте, что школьник подключился к бесплатному Wi-Fi в кафе и решил зайти в социальную сеть. Если точка коннекта небезопасна, мошенники могут получить логин и пароль, а затем взломать аккаунт. Еще одна опасность – вредоносное программное обеспечение, которое способно незаметно загрузиться на устройство, когда оно подключено к незащищенной сети.

Чтобы безопасно пользоваться публичными сетевыми точками, нужно соблюдать несколько правил. Во-первых, не входить в важные аккаунты, такие как банковские приложения или соцсети, если нет уверенности в безопасности сетевой точки. Во-вторых, всегда отключать автоматическое подключение к Wi-Fi, чтобы телефон не подключался к неизвестным сетям без ведома владельца. В-третьих, использовать VPN – специальную программу, которая шифрует интернет-трафик и делает его недоступным для злоумышленников.

Техническая защита – важный аспект цифровой безопасности. Правильные настройки приватности, надежные пароли и осторожность при использовании публичных сетей помогут избежать множества проблем и защитить личные данные от злоумышленников.

Алгоритмы действий в кризисных ситуациях



Иллюстративное фото / newUROKI.net

План действий при обнаружении утечки личных данных

Утечка личных данных – это ситуация, когда ваши пароли, номера телефонов, адреса или другая важная информация становятся доступными посторонним людям. Такое может случиться из-за взлома аккаунта, потери телефона или заражения вирусами. Например, если кто-то получил доступ к вашему аккаунту в социальной сети и начал рассылать сообщения вашим друзьям от вашего имени, это значит, что ваши данные уже в руках злоумышленников.

Если вы обнаружили утечку, первое, что нужно сделать, – проверить, какие сведения скомпрометированы. Например, если ваш пароль больше не работает, значит, его могли изменить. В этом случае необходимо срочно попытаться восстановить доступ через функцию «Забыли пароль?». Если восстановить доступ удалось, сразу же измените пароль на новый, сложный и уникальный. Кроме того, если один и тот же пароль использовался на других сайтах, его тоже нужно поменять, чтобы злоумышленники не смогли зайти в другие ваши аккаунты.

Второй шаг – проверить, не использовались ли ваши реквизиты в мошеннических схемах. Например, если ваш номер телефона или почта оказались в открытом виде, мошенники могут зарегистрировать на них фальшивые аккаунты или пытаться обмануть ваших друзей, выдавая себя за вас. В этом случае стоит предупредить знакомых, чтобы они не доверяли сообщениям, полученным от вашего имени, и внимательно проверяли отправителя.

Если злоумышленники получили возможность входа в вашу банковскую карту или другим финансовым реквизитам, стоит немедленно заблокировать карту и связаться с банком. Это предотвратит возможные списания денег. Также рекомендуется проверить, не были ли оформлены на ваше имя кредиты или подписки на платные сервисы.

Порядок обращения в правоохранительные органы

Если ваши данные были использованы мошенниками, необходимо обратиться в правоохранительные органы. Например, если вас взломали и от вашего имени начали рассылать угрозы или мошеннические сообщения, это может повлечь за собой серьезные последствия. В таком случае важно быстро зафиксировать факт преступления и подать заявление.

Первый шаг – собрать доказательства. Если ваш аккаунт взломали, сделайте скриншоты подозрительных сообщений, изменений в профиле и любых других следов взлома. Если вам поступают угрозы или вымогательство, тоже фиксируйте эти сообщения. Чем больше доказательств у вас будет, тем легче будет расследовать преступление.

Далее необходимо обратиться в полицию. В России заявления можно подать в отделение МВД или через портал «Госуслуги». В заявлении нужно подробно описать ситуацию: когда произошел инцидент, какие сведения были украдены, какие убытки или опасности возникли. Если инцидент связан с мошенничеством в интернете, можно также обратиться в управление «К» МВД, которое занимается киберпреступлениями.

Кроме полиции, можно обратиться в техническую поддержку социальной сети или сервиса, где произошел взлом. Например, если украли ваш аккаунт в Вконтакте, можно отправить запрос на восстановление. Многие платформы предоставляют инструменты для восстановления и защиты учетных записей, если доказать, что вы – настоящий владелец аккаунта.

Способы получения экстренной психологической помощи

Кризисные случаи, связанные с цифровой безопасностью, могут вызывать сильный стресс. Особенно тяжело бывает, если человек сталкивается с кибербуллингом, шантажом или угрозами. Важно помнить, что в таких случаях можно и нужно обращаться за помощью.

Если вы столкнулись с кибербуллингом, шантажом или угрозами, не стоит замыкаться в себе. Обязательно расскажите об этом взрослым: родителям, учителям или школьному психологу. Например, если кто-то публикует про вас оскорбительные посты или распространяет личные фотографии без вашего согласия, не пытайтесь решить проблему в одиночку. Взрослые помогут вам найти выход из ситуации и защитить ваши права.

Существует несколько организаций, которые оказывают бесплатную психологическую помощь подросткам. В России работает телефон доверия для детей и подростков – 8-800-2000-122. По этому номеру можно анонимно поговорить с психологом и получить поддержку. Также есть онлайн-чаты с психологами, где можно обсудить проблему без необходимости звонка.

Если вас преследуют в интернете или угрожают, стоит немедленно заблокировать человека, который это делает, и не вступать с ним в диалог. Злоумышленники часто пытаются вывести жертву на эмоции, заставить ее испугаться или чувствовать себя виноватой. Важно понимать, что такие угрозы – способ манипуляции, и не поддаваться на них.

В кризисных ситуациях главное – не паниковать и действовать спокойно. Если вы обнаружили утечку данных, постарайтесь быстро восстановить контроль над аккаунтами. Если вас преследуют или угрожают, не оставайтесь с этой проблемой наедине, обращайтесь за помощью. Чем быстрее будут приняты меры, тем меньше будет последствий.

Рефлексия

Друзья, сейчас настал момент, когда нужно оценить свои ощущения и мысли после занятия. Это рефлексия. Подумайте, что вы узнали нового сегодня и как эти знания могут повлиять на ваше поведение в сети.

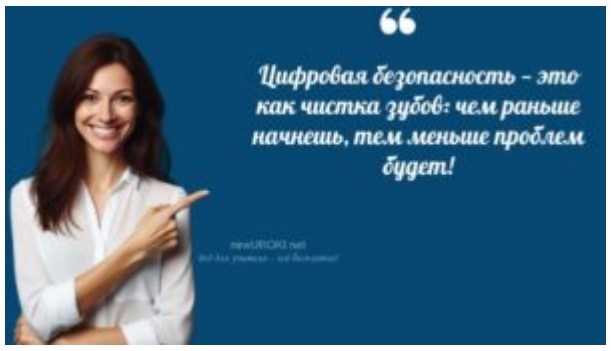
Как вы себя чувствуете после того, как разобрали такие важные темы? Есть ли что-то, что вам было сложно понять, или наоборот, что-то, что оказалось для вас особенно полезным?

Давайте подумаем, как сегодняшняя тема связана с вашим личным опытом. Бывали ли у вас ситуации в интернете, когда вы чувствовали себя неуверенно или сталкивались с опасностью? Возможно, после занятия вы теперь понимаете, как можно было бы избежать этих ситуаций?

Как вы оцениваете свою осведомленность о цифровой безопасности до начала мероприятия и сейчас, после нашего занятия? Напишите в своих мыслях, чему вы научились, а что для вас осталось непонятным. Если есть вопросы, которые вас тревожат, не стесняйтесь их озвучить, мы все вместе постараемся на них ответить.

Эта рефлексия нужна для того, чтобы каждый из вас оценил, насколько важно применять полученные знания, чтобы защищать себя и своих близких в цифровом пространстве. Подумайте, что из сегодняшнего мероприятия вы хотите применить в своей повседневной жизни.

Заключение



Учителя шутят

Уважаемые девятиклассники, сегодня мы не только узнали много нового, но и научились по-настоящему заботиться о своей безопасности в мире, который постоянно меняется. Помните, что каждый из нас может и должен быть внимательным и осмотрительным, независимо от того, используем ли мы интернет для общения, учебы или развлечений.

Ваша активность и стремление защитить себя и своих близких показывают, что вы уже на правильном пути. Применяйте знания, которые вы получили сегодня, не забывайте о своей ответственности, и, конечно, не бойтесь задавать вопросы, если что-то неясно. Все, что вы делаете, направлено на ваше благополучие и успех в этом стремительно развивающемся мире.

Задача каждого из нас — быть не только умным пользователем, но и человеком, который умеет вовремя заметить опасность и с умом с ней справиться. Уверен, что с каждым днем вы будете все лучше разбираться в этом непростом вопросе и становиться более опытными и защищенными.

Давайте продолжать двигаться вперед с оптимизмом, уверенно шагать по пути знания и безопасности, и помните: все в ваших руках!

Домашнее задание

Ученики шутят

Обязательная часть:

- Изучить параграф § и материал учебника
- Составить памятку «Моя безопасность в сети Интернет» (5-7 основных правил)

По желанию:

- Подготовить презентацию об одном из видов интернет-мошенничества и способах защиты от него
- Разработать инфографику по теме «Безопасное общение в социальных сетях»

Технологическая карта

Скачать бесплатно технологическую карту урока по теме: «Правила безопасного поведения 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: «Поведение в цифровой среде» в формате Ворд

Чек-лист педагога

Скачать бесплатно чек-лист для проведения урока ОБЗР по теме: «Поведение в цифровой среде» в формате Word

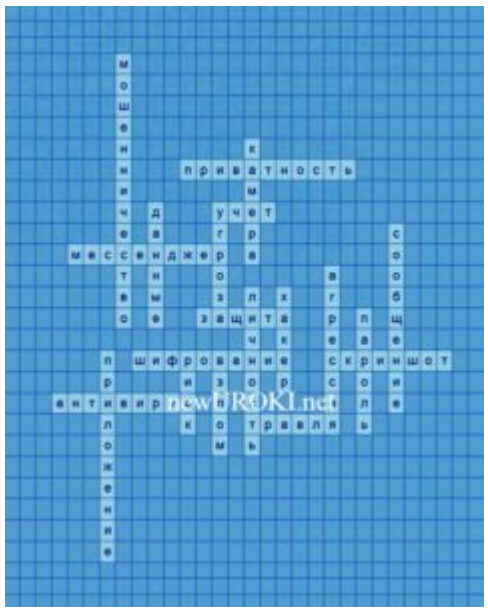
Чек-лист для преподавателя — это инструмент педагогической поддержки, представляющий собой структурированный перечень задач, шагов и критериев, необходимых для успешного планирования, подготовки и проведения урока или мероприятия.

Карта памяти для учеников

Скачать бесплатно карту памяти для учеников 9 класса по ОБЗР по теме: «Поведение в цифровой среде» в формате Ворд

Карта памяти школьника — 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: «Правила безопасного поведения в цифровой среде» в формате WORD

Тесты

Какое действие следует предпринять при получении сообщения с просьбой о финансовой помощи от незнакомого отправителя?
a) Сразу же оказать помощь
b) Проигнорировать сообщение и заблокировать отправителя
c) Вступить в переписку для выяснения деталей
Правильный ответ: b

Что является признаком потенциально опасного сообщества?
a) Наличие открытых комментариев
b) Требование немедленно принять решение
c) Публикация новостей
Правильный ответ: b

Как следует поступить при обнаружении подозрительной рассылки?
a) Переслать друзьям для проверки
b) Открыть все вложения
c) Удалить сообщение без открытия вложений
Правильный ответ: c

Какой пароль считается наиболее надежным?
a) Дата рождения
b) Комбинация букв, цифр и специальных символов
c) Имя домашнего питомца
Правильный ответ: b

При общении с неизвестным пользователем НЕ следует:
a) Использовать вежливые формы общения
b) Сообщать свой домашний адрес
c) Игнорировать неприятные комментарии
Правильный ответ: b

Какой способ является наиболее безопасным для хранения паролей?
a) Записать в блокнот
b) Использовать одинаковый пароль везде
c) Применять специальный менеджер паролей
Правильный ответ: c

При попытке мошенников получить доступ к вашему аккаунту необходимо:
a) Сменить пароль и включить двухфакторную аутентификацию
b) Подождать несколько дней
c) Создать новый аккаунт
Правильный ответ: a

Как правильно реагировать на агрессивные сообщения?
a) Ответить тем же
b) Заблокировать отправителя и сообщить модератору
c) Продолжить общение
Правильный ответ: b

Что следует делать при получении подозрительной ссылки?
a) Перейти по ней в режиме инкогнито
b) Не открывать и удалить сообщение
c) Переслать друзьям для проверки
Правильный ответ: b

Какое действие поможет защитить ваш аккаунт от взлома?
a) Использование простого пароля
b) Привязка номера телефона и почты

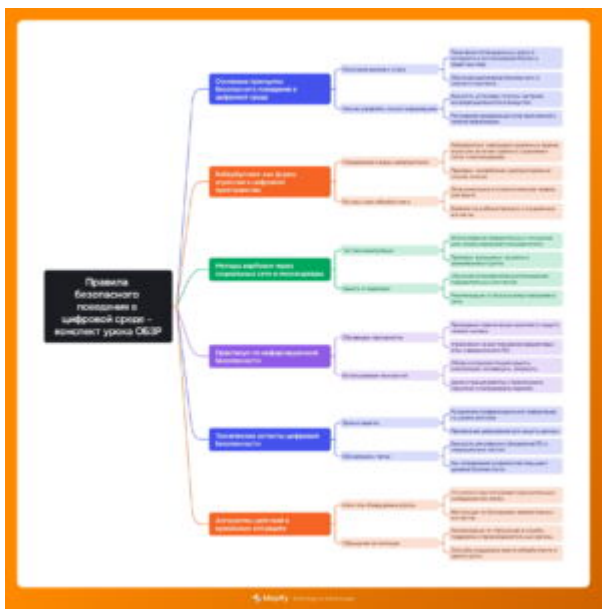
c) Передача пароля друзьям

Правильный ответ: b

Интересные факты для занятия

1. **Интересный факт 1:**
   Каждую минуту в мире создаётся более 300 новых вредоносных программ, и самое удивительное — большинство из них пишутся автоматически, другими программами! Представьте себе фабрику, где роботы собирают других роботов, только в нашем случае — это программы, создающие новые вредоносные программы.
2. **Интересный факт 2:**
   В 2023 году средний подросток тратил на общение в мессенджерах около 7 часов в день — это больше, чем на сон! Получается, что современный школьник проводит в виртуальном общении времени больше, чем средневековый человек тратил на все социальные контакты за неделю. Это кардинально меняет способ формирования дружеских связей и социальных навыков.
3. **Интересный факт 3:**
   Психологи выяснили интересную закономерность: человек склонен доверять сообщениям, написанным с ошибками, больше, чем грамотным текстам. Это связано с тем, что наш мозг воспринимает неидеальный текст как более «человечный» и искренний. Именно поэтому мошенники часто специально делают ошибки в своих сообщениях, чтобы вызвать доверие у получателя.

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

Скачать бесплатно презентацию на урок ОБЗР в 9 классе по теме: «Правила безопасного поведения в цифровой среде» в формате PowerPoint

БОНУС: Рабочий лист

Скачать бесплатно рабочий лист по ОБЗР по теме: «Правила безопасного поведения 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.П. «Основы безопасного поведения в информационной среде». Издательство «Типография 27», Москва, 2004. 215 страниц.
2. Вулевский В.С., Сидоров Н.М. «Методы защиты и предосторожности в современных условиях». Издательство «Сириус», Санкт-Петербург, 2002. 189 страниц.
3. Дерехов И.О. «Основы безопасности и правила защиты». Издательство «Учебная книга», Новосибирск, 2005. 230 страниц.
4. Воронов Е.Г., Андреев Л.В. «Опасности и угрозы: как их распознать и избежать». Издательство «Друзья», Екатеринбург, 2001. 175 страниц.
5. Михайлова Т.А. «Безопасность в повседневной жизни». Издательство «Советский учитель», Ростов-на-Дону, 2003. 198 страниц.

Слова ассоциации (тезаурус) к уроку: шифрование, кибератака, пароль, защита, мониторинг, идентификация, взлом, риск, агрессия, учет

Деструктивные течения в интернете — конспект урока »

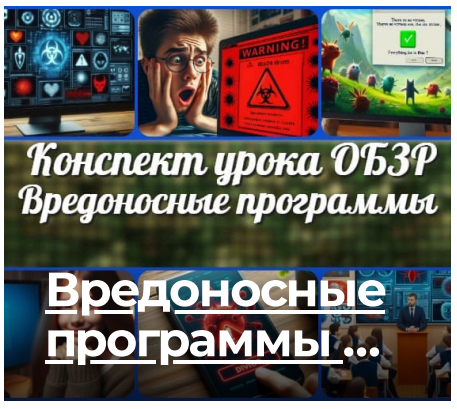
Автор Глеб Беломедведев

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

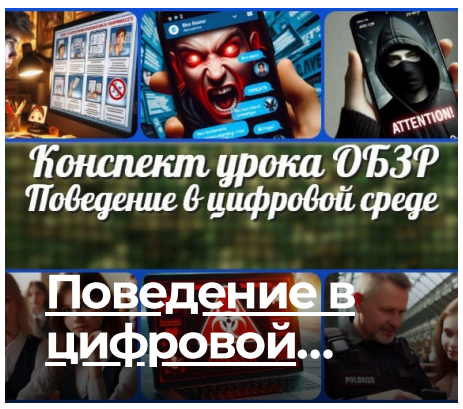
Деструктивны е течения в...

Опасный и запрещенны...

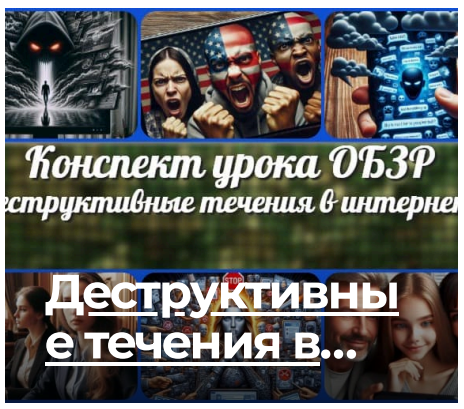


Вредоносные программы ...

ИНТЕРЕСНЫЕ КОНСПЕКТЫ УРОКОВ

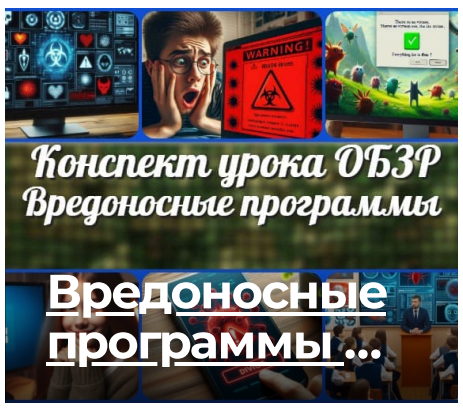


Поведение в цифровой...



Деструктивны е течения в...

Опасный и запрещенны...



Вредоносные программы ...

Новые УРОКИ

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