Новые УРОКИ

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

11 КЛАСС ОБЗР

Безопасность в цифровой среде — конспект урока

Автор Глеб Беломедведев

ЯНВ 16, 2025 #безопасность, #видео, #вирус, #данные, #защита, #интеллект-карта, #интересные факты, #Интернет, #информация, #карта памяти, #кроссворд, #ментальная карта, #облако слов, #полезные советы, #презентация, #признаки, #рабочий лист, #роль, #таблица, #тесты, #технологическая карта, #угроза, #цифровая, #чек-лист 19 фото Время прочтения: 34 минут(ы)

Содержание [Скрыть]

Безопасность в цифровой среде — конспект урока ОБЗР (Основы безопасности и защиты Родины)

Вступление

> ***В эпоху, когда смартфон стал продолжением руки, а виртуальное общение порой заменяет реальное, каждый педагог сталкивается с вызовом: как научить подростков выживать в джунглях цифрового мира? Этот конспект – не просто набор теоретических знаний, а практическое руководство по формированию культуры цифровой безопасности. В материалах вы найдете интерактивную презентацию, технологическую карту урока, тематический кроссворд, тесты и рабочие листы для учащихся, а также актуальные кейсы из жизни современных подростков.***

История
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
ИНТЕРЕСНОЕ

Выберите похожие названия

- Методическая разработка: «Цифровая гигиена современного человека»
- Интегрированное занятие: «Информационная безопасность в эпоху цифровизации»
- Практикум: «Защита личности в виртуальном пространстве»
- Открытый урок: «Цифровые угрозы и методы противодействия им»

Возраст учеников

16-17 лет

Класс

11 класс

Календарно-тематическое планирование

КТП по ОБЗР 11 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 элементами дискуссии

Цель

- Формирование у обучающихся компетенций безопасного поведения в цифровой среде и навыков защиты от информационных угроз

Задачи

- **Обучающая:** сформировать представление о цифровой среде, её компонентах и потенциальных угрозах
- **Развивающая:** развить навыки критического мышления при работе с цифровыми ресурсами
- **Воспитательная:** воспитать ответственное отношение к личной информационной безопасности

Универсальные учебные действия

- **Личностные УУД:** формирование ответственного отношения к собственной информационной защищённости
- **Регулятивные УУД:** развитие умений планировать свои действия в электронной среде
- **Познавательные УУД:** освоение способов безопасной работы с информацией
- **Коммуникативные УУД:** развитие навыков защищённого сетевого взаимодействия
- **Метапредметные УУД:** формирование электронной грамотности

Методические приёмы, педагогические методы, технологии обучения

- Кейс-метод
- Интерактивный диалог
- Работа в малых группах
- Ситуационный анализ
- Мозговой штурм

Ожидаемые результаты

- **Личностные:** осознание значимости информационной защищённости
- **Метапредметные:** умение анализировать информационные угрозы
- **Предметные:** владение основными методами защиты в цифровой среде

Предварительная работа педагога

- Подготовка презентации по теме
- Разработка кейсов с примерами киберугроз
- Создание рабочих листов для практической работы
- Подготовка теста
- Разработка технологической карты
- Создание кроссворда
- Поиск видеоуроков и видеороликов

Оборудование и оформление кабинета

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

Ход занятия / Ход мероприятия

Организационный момент

Здравствуйте, ребята! Давайте проверим, все ли сегодня присутствуют на занятии.

(Проводит перекличку по журналу)

Прошу дежурных подготовить проекционный экран для нашей работы. Анна и Дмитрий, пожалуйста.

А теперь проверим вашу готовность к уроку. Положите на парту учебник, тетрадь и ручку. У всех есть необходимые материалы? Если что-то забыли – поделитесь с соседом по парте.

Посмотрите, пожалуйста, друг на друга – все ли готовы к занятию? Поправьте форму, если необходимо. Рукава рубашек должны быть застёгнуты, девочки – заколите волосы, если они мешают.

Напоминаю правила поведения на уроке: поднимаем руку, если хотим ответить; не перебиваем одноклассников; уважаем мнение каждого. Во время дискуссии высказываемся по очереди. И самая важная просьба – достаньте, пожалуйста, свои телефоны и переведите их в беззвучный режим. Уберите их в сумки до конца занятия. Они нам не понадобятся.

Я вижу ваши улыбки – это замечательно! Какие вы сегодня бодрые и энергичные. Уверен, что наше занятие будет интересным и познавательным. Кстати, кто может рассказать, какое хорошее событие произошло с ним вчера или сегодня утром?

(Выслушивает 2-3 коротких позитивных истории от учеников)

Отлично! Такой позитивный настрой поможет нам продуктивно поработать. Готовы начать? Тогда приступим!

Актуализация усвоенных знаний

Ребята, на прошлом занятии мы с вами изучали очень важную тему – психологические механизмы воздействия на большие группы людей. Давайте вместе вспомним ключевые моменты.

Алексей, расскажи что такое психологическое воздействие и почему оно считается социально-психологическим феноменом? Отлично.

А теперь давайте разберем конкретный пример. Представьте ситуацию: во время футбольного матча болельщики начинают скандировать речёвки и размахивать флагами, постепенно увлекая за собой весь стадион. Маргарита, какой механизм психологического воздействия проявляется в этом случае? Правильно – механизм психологического заражения.

Кто может привести пример использования механизма убеждения в повседневной жизни? Дмитрий, пожалуйста.

А теперь небольшой блиц-опрос. Я буду называть характеристики, а вы поднимаете руку, если это относится к внушению как форме психологического воздействия:

- Основано на критическом осмыслении?
- Имеет скрытый характер воздействия?
- Опирается на готовые аргументы?
- Требует активного участия сознания?

Елена, приведи пример подражания в контексте группового взаимодействия из своего опыта или наблюдений.

И последний вопрос: какие деструктивные психологические технологии воздействия вы можете назвать? Почему они считаются опасными? Кирилл, поделись своими мыслями. Замечательно!

Я вижу, что материал прошлого занятия вы усвоили хорошо. Эти знания будут особенно полезны для понимания новой темы, к которой мы сейчас перейдём.

Вступительное слово учителя

Одиннадцатиклассники, каждый день вы пользуетесь смартфонами, общаетесь в социальных сетях, играете в онлайн-игры, ищете информацию в интернете. Современный мир невозможно представить без цифровых технологий. Но задумывались ли вы когда-нибудь, насколько безопасно ваше путешествие по цифровому пространству?

Приведу пример: представьте, что цифровой мир – это огромный город. В нем есть свои улицы-сайты, дома-приложения, площади-соцсети. И как в любом городе, здесь есть не только добропорядочные жители, но и те, кто может причинить вред. Как вы думаете, что нужно знать и уметь, чтобы безопасно жить в таком городе?

(Выслушивает 2-3 ответа учащихся)

Очень интересные мысли! Именно поэтому сегодняшняя **тема нашего урока – «Безопасность в цифровой среде»**. Запишите, пожалуйста, тему в тетрадях. На этом занятии мы с вами:

- разберемся, что такое электронная среда и какие опасности в ней существуют
- научимся распознавать различные виды информационных угроз
- освоим основные правила безопасного поведения в диджитал-пространстве
- узнаем, как защитить свои персональные данные • поймем, как не стать жертвой кибермошенников

> ***Цитата:***
> ***«Современные технологии могут быть друзьями или врагами, и мы сами решаем, с кем заключать союз.»***
> ***— Г.А. Уховский, 1945–2018, советский инженер, изобретатель, популяризатор науки***

И главное – все эти знания вы сможете сразу же применить в своей повседневной жизни, чтобы сделать свое пребывание в цифровом мире максимально безопасным и комфортным. Готовы отправиться в путешествие по цифровому миру и узнать его секреты? Тогда начинаем!

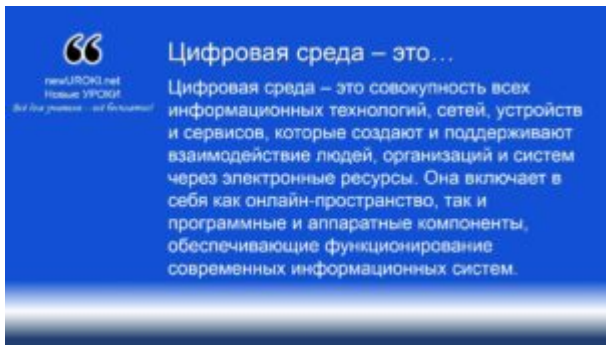
Основная часть

Иллюстративное фото / newUROKI.net

Цифровая среда и ее роль в современном мире

Определение понятия

> ***Цифровая среда – это** совокупность всех информационных технологий, сетей, устройств и сервисов, которые создают и поддерживают взаимодействие людей, организаций и систем через электронные ресурсы. Она включает в себя как онлайн-пространство, так и программные и аппаратные компоненты, обеспечивающие функционирование современных информационных систем.*



Определение

Компоненты современной цифровой среды

Современная информационная экосистема состоит из множества взаимосвязанных элементов, которые обеспечивают её работу.

Основные компоненты:

- **Интернет и локальные сети.** Это базовая инфраструктура для передачи данных, объединяющая пользователей и устройства по всему миру.
- Цифровые устройства. К ним относятся смартфоны, компьютеры, планшеты, а также устройства «умного дома» и носимые гаджеты, которые помогают людям работать, учиться и общаться.
- **Программное обеспечение.** Это операционные системы, приложения и онлайн-сервисы, которые делают возможным взаимодействие между пользователями и информацией.
- **Данные.** Огромные массивы сведений, включая текстовые документы, изображения, видео, аудиофайлы и базы данных, которые создаются и обрабатываются ежедневно.
- **Облачные технологии.** Они обеспечивают доступ к информации и программам через интернет, делая возможной удалённую работу и хранение файлов.
- **Социальные платформы и мессенджеры.** Эти ресурсы объединяют людей, предоставляя инструменты для общения и обмена информацией.
- **Системы защиты и шифрования.** Технологии, которые обеспечивают конфиденциальность и безопасность данных.

Инфографика / newUROKI.net

Влияние цифровизации на различные сферы жизни человека

Информационные технологии глубоко проникли в повседневную жизнь, изменив её практически во всех аспектах:

- **Образование.** Современные школы и вузы активно используют онлайн-платформы для дистанционного обучения, что делает образование доступным независимо от местоположения ученика. Видеоуроки, интерактивные тесты и цифровые учебники стали обычным инструментом обучения.
- **Работа и экономика.** Переход на удалённую работу стал возможен благодаря технологиям видеоконференций и совместного использования информации. Бизнес использует аналитику больших данных и автоматизацию для повышения эффективности.
- **Медицина.** Телемедицина, электронные карты пациентов и автоматизированные системы диагностики облегчают доступ к медицинским услугам и улучшают их качество.
- **Социальное взаимодействие.** Люди поддерживают связь через социальные сети, мессенджеры и видеозвонки, что стало особенно важно в условиях пандемии.
- **Развлечения.** Сервисы потокового видео, игровые платформы и музыкальные приложения предоставляют широкий выбор контента, доступного в любое время.
- **Государственное управление.** Электронные госуслуги позволяют гражданам получать справки, подавать заявления и оплачивать услуги онлайн, упрощая взаимодействие с государственными структурами.

Однако наряду с преимуществами, распространение технологий привело к новым вызовам:

- Усиление зависимости от гаджетов.
- Угроза киберпреступности.
- Проблемы конфиденциальности личной информации.

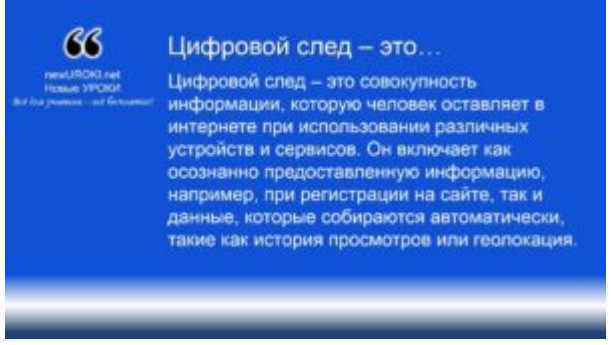
Важно осознавать, что информационная среда стала неотъемлемой частью жизни человека. Задача каждого – учиться использовать её возможности с пользой и минимизировать риски.

Цифровой след и персональные данные

Иллюстративное фото / newUROKI.net

Понятие и виды цифрового следа

> ***Цифровой след – это*** *совокупность информации, которую человек оставляет в интернете при использовании различных устройств и сервисов. Он включает как осознанно предоставленную информацию, например, при регистрации на сайте, так и данные, которые собираются автоматически, такие как история просмотров или геолокация.*



Определение

Цифровой след делится на два вида:

- **Активный.** Это сведения, которые человек осознанно публикует в интернете: комментарии, фотографии, посты в социальных сетях, заполненные анкеты и формы.
- **Пассивный.** Параметры, собираемые автоматически, без активного участия пользователя. Примеры: IP-адрес, история посещения сайтов, время подключения к сети, сведения о местоположении.

Стоит прочесть также: Первая помощь - конспект урока

Категории персональных данных

Персональная информация – это любые сведения, которые позволяют идентифицировать человека.

Она делится на несколько категорий:

- **Основные идентификационные данные.** Фамилия, имя, отчество, дата и место рождения.
- **Контактная информация.** Телефонные номера, электронная почта, адрес проживания.
- **Финансовая информация.** Номера банковских карт, реквизиты счетов, факты о покупках.
- **Чувствительные данные.** Сведения о здоровье, религиозных или политических убеждениях.
- **Биометрическая информация.** Отпечатки пальцев, скан радужки глаза, голосовые записи.
- **Данные о цифровой активности.** История поиска, поведенческие паттерны, использование приложений.

Инфографика / newUROKI.net

Эти сведения имеют ценность для злоумышленников, рекламодателей и аналитических компаний, поэтому важно понимать, как они могут быть использованы.

Правовые основы защиты персональных данных

Защита личной информации регулируется законами и международными соглашениями. В Российской Федерации действует Федеральный закон No 152-ФЗ «О персональных данных».

Основные положения:

- **Сбор только с согласия пользователя.** Организации обязаны получать разрешение на обработку этих фактов.
- **Хранение в условиях конфиденциальности.** Доступ к материалам должны иметь только уполномоченные лица.
- **Целевое использование.** Личные сведения могут использоваться только для тех целей, которые указаны при их сборе.
- **Право на удаление.** Пользователь может потребовать удаления своих материалов из системы.
- **Ответственность за нарушение.** Штрафы и уголовная ответственность для организаций и лиц, нарушивших закон.

В международной практике действует Общее положение о защите данных (GDPR) в странах ЕС, которое также регулирует вопросы обработки и хранения личной информации.

Почему важно защищать личные сведения?

В современном мире любая утечка может стать причиной серьёзных проблем:

- Финансовые потери из-за мошеннических действий.
- Нарушение приватности и репутации.
- Использование материалов для манипуляций и шантажа.

Чтобы минимизировать риски:

- Ограничивайте количество фактов, предоставляемых в интернете.
- Используйте надёжные пароли и двухфакторную аутентификацию.
- Устанавливайте антивирусные программы и регулярно обновляйте их.
- Будьте внимательны при заполнении форм на неизвестных сайтах.

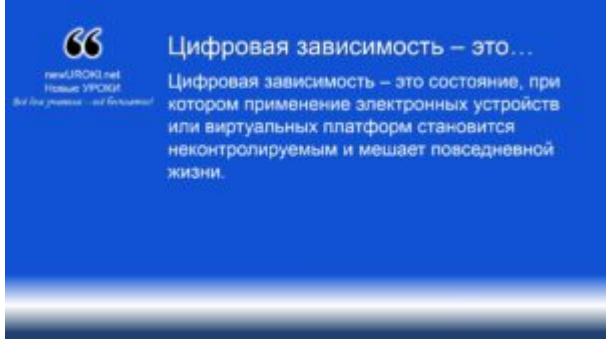
Соблюдение этих правил поможет сохранить вашу приватность и обезопасить вашу активность в информационной среде.

Цифровая зависимость как современная угроза

Иллюстративное фото / newUROKI.net

Определение и признаки

> ***Цифровая зависимость – это** состояние, при котором применение электронных устройств или виртуальных платформ становится неконтролируемым и мешает повседневной жизни.*



Определение

Признаки этого состояния включают:

- **Постоянное стремление быть в сети.** Человек проверяет социальные сети, сообщения или электронную почту даже без явной необходимости.
- **Снижение интереса к реальным событиям.** Общение с друзьями, хобби или учеба теряют значимость по сравнению с виртуальной активностью.
- **Эмоциональная аддикция*.** Человек испытывает тревогу или раздражение, если лишён доступа к интернету или гаджетам.
- **Потеря контроля над временем.** Использование устройств занимает больше времени, чем планировалось, из-за чего откладываются важные дела.
- **Снижение продуктивности.** Ухудшение концентрации внимания, снижение академической успеваемости или производительности на работе.

> ***Аддикция** (зависимость) (англ. addiction — зависимость, пагубная привычка, привыкание), в широком смысле, — ощущаемая человеком навязчивая потребность в определённой деятельности. Рувики*

Инфографика / newUROKI.net

Психологические и физиологические последствия

Длительное и неконтролируемое применение технологий может привести к серьёзным проблемам.

Психологические последствия:

- **Ухудшение эмоционального состояния.** Частое пребывание в сети может вызывать раздражительность, тревожность, апатию и даже депрессию.
- **Снижение способности к реальному взаимодействию.** Навыки межличностного общения ослабевают, возникают трудности в построении живых отношений.
- **Развитие синдрома упущенной выгоды (FOMO).** Человек испытывает постоянный страх пропустить важную новость или событие в интернете.
- **Повышенная импульсивность.** Потребность от мгновенной обратной связи в сети может привести к нетерпеливости и снижению способности к долгосрочному планированию.

Физиологические последствия:

- **Проблемы со зрением.** Длительное время перед экраном приводит к перенапряжению глаз и синдрому «сухого глаза».
- **Нарушение сна.** Яркий экран гаджетов перед сном нарушает выработку мелатонина, что приводит к бессоннице.

- **Боли в спине и шее.** Неправильная осанка при использовании устройств вызывает мышечное напряжение и хронические боли.
- **Снижение физической активности.** Долгое пребывание за компьютером или смартфоном увеличивает риск ожирения и сердечно-сосудистых заболеваний.

Методы профилактики и преодоления цифровой зависимости

Проблема несвободности от технологий требует комплексного подхода, который включает как профилактические меры, так и способы её устранения.

Методы профилактики:

- **Ограничение времени.** Установите чёткие временные рамки для использования устройств. Программы тайм-менеджмента и родительский контроль могут помочь в этом.
- **Развитие хобби.** Найдите увлечение, которое не связано с эксплуатацией гаджетов: спорт, музыка, творчество или чтение книг.
- **Режим дня.** Соблюдайте баланс между виртуальной активностью, учёбой, работой и отдыхом.
- **Время без экранов.** Выделяйте часы, в которые использование смартфонов и других устройств запрещено, например, за ужином или перед сном.

Методы преодоления:

- **Психологическая поддержка.** Обращение к психологу или консультанту может помочь понять причины такой несвободности и найти пути её преодоления.
- **Детокс от технологий.** Временное отключение от интернета или социальных сетей помогает восстановить баланс между виртуальной и реальной жизнью.
- **Осознанное использование технологий.** Научитесь задавать себе вопрос: «Зачем я сейчас беру в руки телефон или включаю компьютер?»
- **Вовлечение близких.** Попросите друзей или родственников помочь вам контролировать время, проведённое за экраном.

Осознание проблемы и работа над её устранением помогут не только улучшить качество жизни, но и избежать долгосрочных негативных последствий. Сохранение равновесия между реальной и виртуальной активностью – важный шаг к здоровому образу жизни.

Основные угрозы в цифровой среде

Иллюстративное фото / newUROKI.net

Вредоносное программное обеспечение

Вредоносное программное обеспечение – это программы, которые создаются с целью нарушения работы устройств, кражи личных данных или получения несанкционированного доступа к системам.

Основные виды вредоносных программ:

- **Вирусы.** Программы, которые распространяются, прикрепляясь к файлам или приложениям, и наносят ущерб системе, повреждая данные или замедляя работу устройств. Пример: вирус, удаляющий файлы с компьютера.
- **Троянские программы.** Эти приложения маскируются под полезные приложения, но после установки на устройство предоставляют злоумышленникам доступ к системе. Пример: «бесплатный антивирус», который крадёт пароли.
- **Шпионское ПО.** Оно собирает информацию о пользователе без его ведома, например, логины, пароли или историю поиска.
- **Вымогатели.** Утилиты, которые шифруют файлы на устройстве и требуют выкуп за их восстановление. Например: известный вирус **WannaCry***.
- **Черви.** Они распространяются автономно, без необходимости прикрепления к файлам, и могут выводить из строя целые сети.

> ***WannaCry — вредоносная программа, сетевой червь и программа-вымогатель денежных средств, поражающая компьютеры под управлением операционной системы Microsoft Windows. Википедия***

Как защититься от вредоносных утилит:

- Установить антивирусное ПО и регулярно обновлять его.
- Загружать приложения только из официальных магазинов.
- Не открывать подозрительные файлы, полученные по электронной почте.
- Создавать резервные копии данных.

Методы социальной инженерии и сетевого мошенничества

Социальная инженерия – это способы обмана, при которых злоумышленники манипулируют людьми, чтобы получить доступ к конфиденциальным данным.

Основные методы социальной инженерии:

- **Фишинг.** Пользователю отправляют электронное письмо или сообщение, которое выглядит как официальное, с просьбой предоставить личные данные, например, пароли. Например: сообщение якобы от банка с просьбой подтвердить номер карты.
- **Вишинг.** Мошенничество по телефону, когда злоумышленники выдают себя за сотрудников служб поддержки или банков.
- **Смишинг.** Использование SMS-сообщений для получения конфиденциальной информации. Например, сообщение о «выигрыше» с просьбой перейти по ссылке.
- **Псевдотехподдержка.** Злоумышленники представляются специалистами службы поддержки и просят установить программу, которая позволяет им управлять устройством удалённо.

Как защититься от социальных манипуляций:

- Не передавать личную информацию незнакомцам, даже если они кажутся убедительными.
- Проверять ссылки, прежде чем переходить по ним (например, обратить внимание на домен сайта).
- Использовать сложные пароли и не сообщать их никому.

Кибербуллинг и деструктивные сообщества

Кибербуллинг – это форма травли, которая осуществляется через интернет. Это может быть оскорбление, распространение слухов, угрозы или унижение с использованием социальных сетей, мессенджеров или форумов.

Примеры кибербуллинга:

- Публикация в сети фотографий человека с оскорбительными подписями.
- Распространение ложной информации с целью опозорить человека.

- Массовая отправка негативных комментариев или сообщений.

Деструктивные сообщества – это группы в интернете, которые склоняют участников к опасным действиям.

Примеры таких сообществ:

- Группы, поощряющие участие в опасных «челленджах» (например, выполнение опасных трюков).
- Сообщества, пропагандирующие ненависть или насилие.
- Группы, в которых подстрекают к самоповреждениям.

Как защититься от кибербуллинга и влияния опасных групп:

- Настроить конфиденциальность в социальных сетях, ограничив доступ к информации о себе.
- Игнорировать провокационные комментарии и блокировать обидчиков.
- Сообщать о кибербуллинге или подозрительных группах взрослым или в службу поддержки платформы.

Пример из жизни: ученица одной школы стала жертвой кибербуллинга после неудачного выступления на школьном конкурсе. В её адрес начали поступать оскорбительные комментарии. После того как она обратилась к школьному психологу, травля прекратилась, а обидчики понесли ответственность.

Внимательное отношение к собственной безопасности в сети и следование базовым правилам помогут избежать многих угроз и сохранить спокойствие.

Таблица: Основные угрозы и способы защиты

Угроза	Способ защиты
Вредоносное ПО	Антивирусные программы
Кража личных сведений	Шифрование пакетов
Мошенничество в интернете	Обучение безопасному поведению
Атаки с использованием фишинга	Проверка источников информации
Кибербуллинг	Блокировка и игнорирование агрессоров

Информационная безопасность личности

Иллюстративное фото / newUROKI.net

Принципы защиты личной информации

Информационная безопасность личности заключается в обеспечении сохранности персональных сведений и недопущении их использования без согласия владельца.

Основные принципы защиты:

- **Минимизация раскрытия данных.** Делитесь только той информацией, которая необходима в конкретной ситуации. Пример: при регистрации на сайте указывайте только обязательные сведения, такие как имя и адрес электронной почты, избегая заполнения необязательных полей.
- **Контроль за доступом.** Настраивайте уровни конфиденциальности в социальных сетях, чтобы ограничить круг лиц, которые могут видеть ваши публикации. Например, личные фото могут быть доступны только друзьям, а не всем пользователям интернета.
- **Осознанное поведение.** Прежде чем размещать сведения в интернете, подумайте, могут ли они быть использованы против вас.

Пример: не стоит публиковать сведения о своём местоположении в режиме реального времени.

Регулярное обновление знаний. Будьте в курсе актуальных угроз и способов предохранения от них.

Методы обеспечения конфиденциальности данных

Сохранение конфиденциальности подразумевает применение различных мер для защиты информации от утечки или несанкционированного доступа.

Методы обеспечения безопасности:

- **Сложные пароли.** Используйте пароли длиной не менее 12 символов, которые включают буквы, цифры и специальные символы. Например: вместо пароля «123456» можно создать «P@ssw0rd2023!».
- **Двухфакторная аутентификация (2FA).** Этот метод добавляет дополнительный уровень безопасности. Например, при входе в аккаунт, помимо пароля, необходимо ввести код из SMS или приложения.
- **Шифрование данных.** Использование программ для шифрования файлов защищает информацию от несанкционированного доступа. Пример: приложения, такие как VeraCrypt, создают зашифрованные хранилища.
- **Антивирусное программное обеспечение.** Оно предотвращает заражение устройств вредоносными программами. Регулярно обновляйте антивирус, чтобы защититься от новых угроз.
- **Избегание публичных Wi-Fi.** Подключение к открытым сетям может привести к утечке данных. Если необходимо подключиться к общедоступному Wi-Fi, используйте VPN для шифрования трафика.

Стоит прочесть также: Психологическое благополучие - конспект урока

Инструменты цифровой безопасности

Для повышения уровня защиты существуют специализированные программы и сервисы, которые делают использование интернета более безопасным.

Примеры инструментов:

- **Менеджеры паролей.** Программы, которые сохраняют все ваши пароли и помогают создавать уникальные комбинации. Пример: LastPass, 1Password.
- **VPN (виртуальная частная сеть).** Шифрует интернет-трафик, защищая его от перехвата. Например, при эксплуатации VPN ваш IP-адрес скрывается, что повышает анонимность.
- **Антивирусы.** Kaspersky, Norton и другие программы помогают выявлять и блокировать угрозы.
- **Блокировщики рекламы.** Некоторые рекламные баннеры содержат вредоносные скрипты. Инструменты вроде AdBlock защищают пользователя от таких рисков.

- **Контроль доступа.** Настройте на устройствах PIN-коды, биометрическую идентификацию (например, отпечаток пальца), чтобы ограничить доступ к вашим материалам.
- **Файрволы.** Защитные программы, которые фильтруют входящий и исходящий трафик, предотвращая несанкционированный доступ.

Пример из жизни:
Одна из учениц заметила, что её страница в социальной сети была взломана. Злоумышленники рассылали сообщения её друзьям с просьбой перевести деньги. После консультации с учителем она изменила пароль на более сложный, включила двухфакторную аутентификацию и установила антивирус, что помогло предотвратить дальнейшие взломы.

Следование этим принципам и использование указанных инструментов помогут создать надёжную защиту информации, снизив вероятность её утраты или злоупотребления.

Культура безопасного поведения в цифровой среде

Иллюстративное фото / newUROKI.net

Правила безопасного использования цифровых устройств

Эффективное и безопасное использование технологий начинается с соблюдения базовых правил. Они помогут избежать утраты личной информации, кибератак и других рисков.

Основные правила:

- Регулярное обновление программного обеспечения. Устаревшие версии программ и операционных систем часто имеют уязвимости, которые могут быть использованы злоумышленниками. Пример: настройте автоматические обновления для смартфонов и компьютеров.
- Создание сложных паролей. Никогда не используйте простые комбинации, такие как «123456». Замените их на фразы, которые трудно угадать, например: «M@yD@y2023!».
- Ограничение доступа к устройству. Настраивайте блокировку экрана с помощью пароля, отпечатка пальца или распознавания лица.
- Осторожность при установке приложений. Загружайте программы только из проверенных источников, таких как официальные магазины приложений.
- Регулярная проверка подключений. Следите за тем, какие устройства и сети подключены к вашему оборудованию, и отключайте неизвестные соединения.

Пример: Ученик, используя бесплатное приложение для редактирования фотографий, столкнулся с постоянной рекламой и всплывающими окнами. Оказалось, что приложение собирает сведения о пользователях. После удаления программы и установки антивируса проблема была решена.

Алгоритмы действий при столкновении с угрозами

Знание конкретных шагов поможет быстро и правильно реагировать на возникающие риски.

Действия при различных угрозах:

Фишинг (мошенничество через электронные письма или сайты):

- Не переходите по подозрительным ссылкам.
- Проверяйте адрес отправителя: настоящие компании не используют электронные почты с подозрительными доменами.
- Если вы ввели персональные данные, немедленно измените пароли и сообщите об инциденте.

Вредоносные программы:

- При подозрении на вирус отключите устройство от интернета.
- Запустите антивирусную проверку.
- Обратитесь за помощью к специалистам.

Кибербуллинг или угрозы:

- Заблокируйте агрессора.
- Сделайте скриншоты переписок.
- Сообщите родителям, учителям или в соответствующие службы.

Пример: Один из учащихся получил письмо с просьбой подтвердить аккаунт, указав личные данные. Предполагая, что это мошенничество, он показал письмо учителю, который подтвердил, что это фишинг. Таким образом, удалось избежать потери учётной записи.

Формирование навыков критического мышления при работе с информацией

Современный пользователь должен уметь анализировать информацию, чтобы отличать достоверные источники от ложных.

Основные навыки:

- Оценка достоверности источника. Прежде чем доверять новости, проверьте, кто её опубликовал и какие цели может преследовать автор. Например, статьи с официальных новостных порталов заслуживают большего доверия, чем посты в социальных сетях.
- Факт-чекинг. Сравнивайте сведения из разных источников. Если новость публикуется только на одном сайте, это повод задуматься о её правдивости.
- Осознанное потребление контента. Не доверяйте информации, которая вызывает сильные эмоции, особенно страх или гнев. Такие материалы часто манипулятивны.

Пример: Одиннадцатиклассник наткнулся в интернете на шокирующую новость, призывающую к определённым действиям. Однако он нашёл противоречивую информацию на других ресурсах и понял, что это фейк.

Формирование культуры безопасного поведения в онлайн-среде требует осознанного подхода, анализа ситуации и применения проверенных методов защиты. Выполнение этих рекомендаций позволяет избежать множества проблем, связанных с использованием современных технологий.

Рефлексия

Дорогие ребята, сейчас давайте подведём итоги нашего занятия и проведём рефлексию.

Оцените своё настроение и состояние:

Закройте глаза на несколько секунд и постарайтесь почувствовать, с каким настроением вы завершаете сегодняшнее занятие. Стали ли вы более уверенными в своих знаниях? Почувствовали ли вы, что теперь можете лучше защищать себя и своё пространство?

Давайте поговорим о том, что нового вы узнали:

Какие моменты урока показались вам наиболее полезными?
Какие советы или рекомендации вы собираетесь применять в повседневной жизни?

Обратная связь.

Возьмите карточки или листки, которые я вам раздал в начале урока. На одной стороне напишите, что вам понравилось и что было самым интересным. На другой стороне напишите, что бы вы хотели уточнить или узнать подробнее в будущем.

Самооценка.

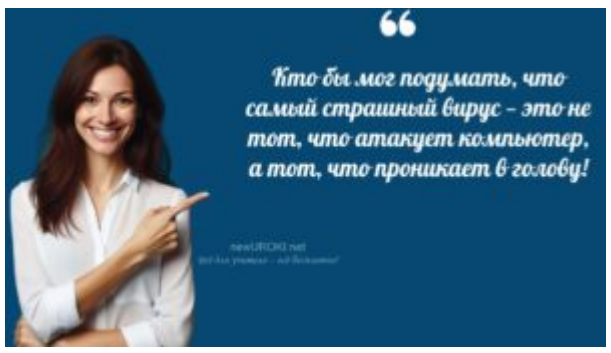
Поднимите руку те, кто:

- Узнал что-то принципиально новое для себя.
- Почувствовал, что уже готов применять полученные знания.
- Задумался о своих привычках или способах работы с информацией.

Метафора для настроения.

Заканчивая занятие, давайте опишем своё состояние одной метафорой. Например: «Я чувствую себя защитником своей информации, словно рыцарь с крепким щитом». А как бы вы описали своё настроение?

Заключение



Учителя шутят

Сегодня мы сделали ещё один шаг к тому, чтобы стать уверенными и компетентными людьми в нашем стремительно меняющемся мире. Вы получили знания, которые помогут вам не только защитить себя, но и почувствовать себя более подготовленными к любым вызовам современности.
Каждый из вас теперь знает, как важно сохранять осознанность, быть внимательными к тому, что нас окружает, и действовать разумно. Помните, что ваше умение анализировать ситуации, предвидеть возможные последствия и принимать взвешенные решения – это настоящий навык, который пригодится вам не только здесь, в школе, но и в вашей дальнейшей жизни.
Вы – поколение, которому предстоит строить будущее. И от того, как вы будете подходить к вопросам своей безопасности и разумного использования современных технологий, зависит не только ваша личная защищённость, но и гармония в обществе.
Я верю в каждого из вас. Вы можете многое, если будете идти вперёд с любопытством, умом и ответственностью. Пусть сегодняшнее занятие станет для вас ещё одной опорой на этом пути. Уверенно смотрите в завтрашний день, применяйте знания на практике и не забывайте делиться ими с окружающими.
Спасибо вам за вашу вовлечённость и стремление к новым открытиям. Вы действительно молодцы!

Домашнее задание

Ученики шутят

- Составить памятку «Правила безопасного поведения в социальных сетях»
- Провести анализ собственного цифрового следа
- (По желанию) Подготовить мини-проект «Моя стратегия информационной безопасности»

Технологическая карта

Скачать бесплатно технологическую карту урока по теме: «Безопасность 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: «Безопасность в цифровой среде» в формате Ворд

Чек-лист педагога

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

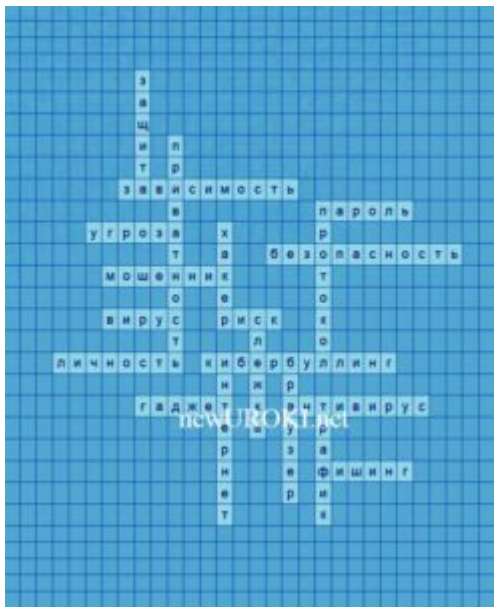
Чек-лист для учителя — это инструмент педагогической поддержки, представляющий собой структурированный перечень задач, шагов и критериев, необходимых для успешного планирования, подготовки и проведения урока или мероприятия.

Карта памяти для учеников

Скачать бесплатно карту памяти для учеников 11 класса по ОБЗР по теме: «Безопасность в цифровой среде» 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 11 классе по теме: «Безопасность в цифровой среде» в формате WORD

Тесты

Какая технология чаще всего применяется злоумышленниками для кражи паролей?

а) Фишинг

б) Майнинг

в) Стриминг

Правильный ответ: а

Как называется навязчивое преследование и травля человека в интернет-пространстве?

а) Троллинг

б) Буллинг

в) Спамминг

Правильный ответ: б

Что рекомендуется делать при получении сообщения от незнакомого отправителя со ссылкой?

а) Перейти по ссылке из любопытства

б) Удалить сообщение не открывая

в) Переслать друзьям для проверки

Правильный ответ: б

Какой пароль считается наиболее надежным?

а) Дата рождения

б) Имя питомца

в) Комбинация букв, символов и чисел

Правильный ответ: в

При обнаружении подозрительной активности на личной странице необходимо:

а) Проигнорировать изменения

б) Немедленно сменить пароль

в) Подождать сутки

Правильный ответ: б

Какое действие является признаком мошеннической схемы?

а) Просьба назвать код из СМС

б) Запрос имени пользователя

в) Уточнение времени встречи

Правильный ответ: а

Как часто рекомендуется менять пароли на важных аккаунтах?

а) Раз в неделю

б) Раз в три месяца

в) Раз в год

Правильный ответ: б

При общении с неизвестным человеком в мессенджере следует:

а) Рассказать о своих планах

б) Поделиться личными фото

в) Ограничить объем личных сведений

Правильный ответ: в

Признаком психологической зависимости от виртуального общения является:

а) Проверка сообщений раз в день

б) Потеря интереса к реальному общению

в) Наличие нескольких аккаунтов

Правильный ответ: б

Для защиты от вредоносных программ необходимо:

а) Регулярно обновлять защитное ПО

б) Отключить антивирус

в) Открывать все вложения

Правильный ответ: а

Интересные факты для занятия

1. **Интересный факт 1:**
   В 2023 году средний подросток тратит на онлайн-активность больше времени, чем на сон — около 9 часов ежедневно. При этом мозг человека способен эффективно воспринимать контент только 4-5 часов в день, после чего начинается снижение концентрации и работоспособности.
2. **Интересный факт 2:**
   Психологи установили, что человек, который постоянно делает селфи и выкладывает их в интернет, подсознательно ищет одобрения окружающих. Это явление назвали «селфитис» — новой формой психологической зависимости. В тяжёлых случаях люди делают более 50 селфи в день.
3. **Интересный факт 3:**
   В 2024 году самым популярным паролем в мире остаётся комбинация «123456», которую можно взломать за доли секунды. На втором месте — слово «password». Эксперты подсчитали, что каждую минуту в мире происходит около 2200 попыток взлома аккаунтов с простыми паролями.

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 11 классе по теме: «Безопасность в цифровой среде» в формате PowerPoint

БОНУС: Рабочий лист

Скачать бесплатно рабочий лист по ОБЗР по теме: «Безопасность 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. Фуковский А.П., «Практическое руководство по анализу систем и структур». Издательство «Технопрогресс», Санкт-Петербург, 2004. 245 страниц.
2. Кузнецова Л.В., Женова И.Н., «Современные подходы к изучению среды взаимодействия». Издательство «Герань», Казань, 2005. 312 страниц.
3. Васильев М.С., «Влияние технологий на привычки и повседневную жизнь». Издательство «Орион», Москва, 2001. 178 страниц.
4. Орлов Е.А., Треевская И.В., «Психология и развитие подростков в условиях перемен». Издательство «Эволюция», Новосибирск, 1999. 264 страницы.

5. Медовой Ю.Н., «Основы работы с современными инструментами». Издательство «Интеграл», Екатеринбург, 2002. 154 страницы.

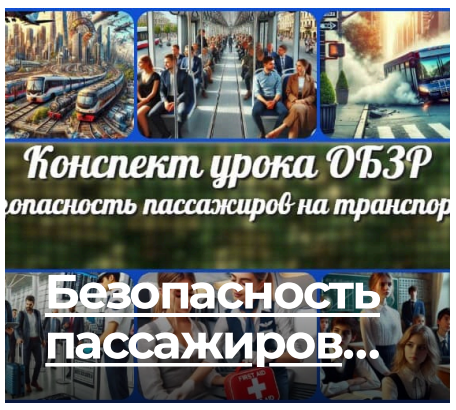
Слова ассоциации (тезаурус) к уроку: угроза, защита, приватность, уязвимость, хакер, протокол, шифрование, контроль, угрозы, средства, конфиденциальность.

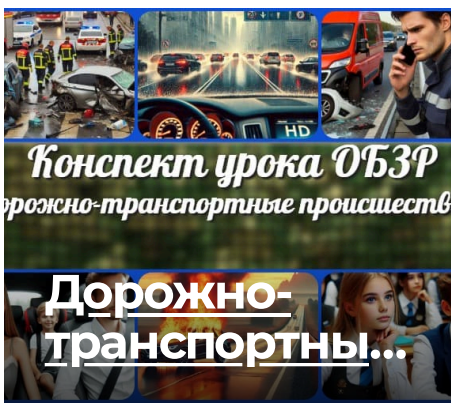
Помощь при ЧС на транспорте — конспект урока »

Автор Глеб Беломедведев

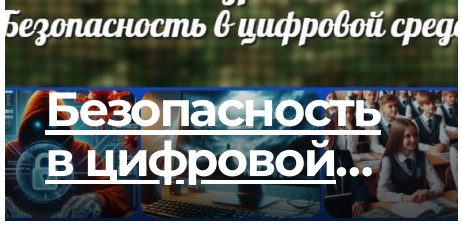
Глеб Беломедведев - постоянный автор и эксперт newUROKI.net, чья биография олицетворяет трудолюбие, настойчивость в достижении целей и экспертность. Он обладает высшим образованием и имеет более 5 лет опыта преподавания в школе. В течение последних 18 лет он также успешно работает в ИТ-секторе. Глеб 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

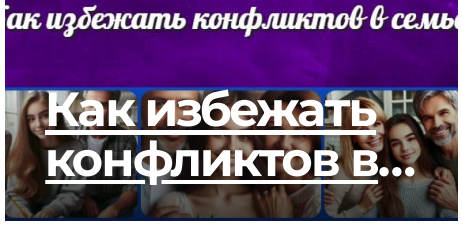




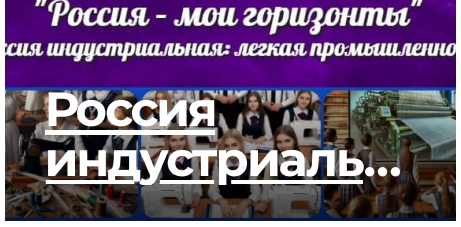
ИНТЕРЕСНЫЕ КОНСПЕКТЫ УРОКОВ



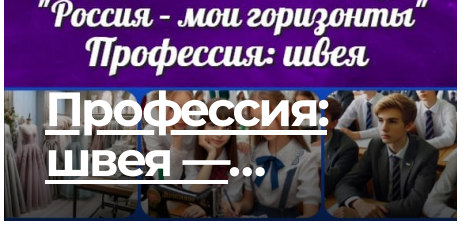
Безопасность в цифровой...



Как избежать конфликтов в...



Россия индустриаль...



Профессия: швея —...

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