Новые УРОКИ

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

11 КЛАСС ОБЗР

Защита прав в цифровом пространстве — конспект урока

Автор Глеб Беломедведев

ЯНВ 22, 2025 #видео, #государство, #данные, #закон, #защита, #интеллект-карта, #интересные факты, #Интернет, #информация, #карта памяти, #кроссворд, #ментальная карта, #метод, #облако слов, #ответственность, #полезные советы, #правила, #право, #правонарушение, #презентация, #рабочий лист, #Россия, #таблица, #тесты, #технологическая карта, #цифровая, #чек-лист, #человек 18 фото Время прочтения: 34 минут(ы)

Содержание [Скрыть]

1 Защита прав в цифровом пространстве — конспект урока ОБЗР (Основы безопасности и защиты Родины)
2 Вступление
3 Выберите похожие названия
4 Возраст учеников
5 Класс
6 Календарно-тематическое планирование
7 Модуль
8 УМК (Учебно-методический комплекс)
9 Учебник

Поиск

Поиск

ИНТЕРЕСНОЕ

КОНСПЕКТЫ УРОКОВ

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

10 Дата проведения
11 Длительность
12 Вид
13 Тип
14 Форма проведения
15 Цель
16 Задачи
17 Универсальные учебные действия (УУД)
18 Методические приёмы, педагогические методы, технологии обучения
19 Ожидаемые результаты
20 Предварительная работа педагога
21 Оборудование и оформление кабинета
22 Ход занятия / Ход мероприятия
22.1 Организационный момент
22.2 Актуализация усвоенных знаний
22.3 Вступительное слово преподавателя-организатора
23 Основная часть
23.1 Права человека в цифровом пространстве
23.2 Безопасность в цифровой среде
23.3 Ответственность за действия в интернете
23.4 Запрещенный контент и правовые последствия
23.5 Механизмы защиты прав в цифровом пространстве
23.6 Практические навыки защиты прав
24 Рефлексия
25 Заключение
26 Домашнее задание
27 Технологическая карта
28 Смотреть видео по теме
29 Полезные советы учителю
30 Чек-лист педагога
31 Карта памяти для учеников
32 Кроссворд
33 Тесты
34 Интересные факты для занятия
35 Интеллект-карта
36 Облако слов
37 Презентация
38 БОНУС: Рабочий лист
39 Список источников и использованной литературы

Защита прав в цифровом пространстве — конспект урока ОБЗР (Основы безопасности и защиты Родины)

Вступление

> ***В эпоху, когда смартфон стал продолжением руки, а виртуальное общение порой затмевает реальное, защита прав в сети приобретает особое значение. Предлагаем вашему вниманию комплексный методический материал, включающий технологическую карту, презентацию, интерактивные тесты, рабочие листы и кроссворд для эффективного проведения занятия по цифровой безопасности. Материал поможет сформировать у старшеклассников критическое мышление и практические навыки защиты в информационном пространстве.***

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 грамотность и информационная безопасность»
- Интегрированное занятие: «Правовая защита в современном информационном обществе»
- Открытый урок: «Безопасность личности в виртуальном пространстве»
- Практикум: «Основы кибербезопасности и защиты цифровых прав»

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 и первичное закрепление новых знаний

Форма проведения

Интерактивное занятие с элементами практической работы

Цель

- Сформировать у обучающихся систему знаний и практических навыков по защите личных прав в цифровом пространстве

Задачи

- **Обучающая:** Сформировать представление о правах человека в цифровой среде и способах их защиты
- **Развивающая:** Развить навыки безопасного поведения в электронной среде и критического мышления
- **Воспитательная:** Воспитать ответственное отношение к своим действиям в информационном пространстве

Универсальные учебные действия (УУД)

- **Личностные УУД:** Формирование ответственного отношения к собственной информационной безопасности
- **Регулятивные УУД:** Развитие умения планировать свои действия в сетевой среде
- **Познавательные УУД:** Освоение способов защиты персональных данных и противодействия киберугрозам
- **Коммуникативные УУД:** Развитие навыков безопасного сетевого взаимодействия
- **Метапредметные УУД:** Формирование навыков применения правовых знаний в интернет-среде

Методические приёмы, педагогические методы, технологии обучения

- Кейс-метод
- Интерактивное обсуждение
- Работа в группах
- Анализ практических ситуаций
- Мозговой штурм

Ожидаемые результаты

- **Личностные:** Осознание важности защиты личных прав в электронном пространстве
- **Метапредметные:** Умение применять правовые знания при использовании электронных технологий
- **Предметные:** Знание основных прав и механизмов их защиты в электронной среде

Предварительная работа педагога

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

Оборудование и оформление кабинета

- Компьютер с доступом в интернет
- Проектор и экран
- Раздаточный материал
- Плакаты
- Рабочие листы для учащихся

Ход занятия / Ход мероприятия

Организационный момент

Здравствуйте, ребята! Прошу всех встать и поприветствовать друг друга.

(Учащиеся встают)

Садитесь, пожалуйста. Начинаем занятие. Сейчас я проведу перекличку, чтобы отметить присутствующих.

(Учитель проводит перекличку по журналу)

Дежурные, пожалуйста, подготовьте проекционный экран для работы. А пока они этим занимаются, все остальные проверьте готовность к занятию. На партах должны быть: рабочая тетрадь, учебник, ручка и карандаш. Уберите со столов все лишние предметы.

Обратите внимание на внешний вид — форма должна быть в порядке. Иванов, поправь, пожалуйста, воротник.

Ребята, прошу всех отключить мобильные телефоны или перевести их в беззвучный режим. Это необходимо для эффективной работы и уважительного отношения друг к другу.

На время занятия у нас действуют стандартные правила: поднимаем руку, если хотим ответить; не перебиваем одноклассников; внимательно слушаем выступающего.

Я вижу, что все готовы к работе. Посмотрите, какой сегодня прекрасный день! Надеюсь, ваше настроение тоже замечательное. Давайте улыбнемся — позитивный настрой очень важен для продуктивной работы.

Дежурные справились с подготовкой экрана? Отлично! Спасибо за помощь.

Вижу, что вы полностью готовы. Рад видеть в ваших глазах интерес и желание получать новые знания. Уверен, сегодняшнее занятие будет очень познавательным и полезным для каждого из вас.

Актуализация усвоенных знаний

Друзья, на прошлом занятии мы с вами изучали очень важную тему — достоверность информации в цифровой среде. Давайте освежим в памяти ключевые моменты. Я задам вам несколько вопросов, а вы постарайтесь дать развернутые ответы.
Петров, расскажи, пожалуйста, какие особенности современной информационной среды мы обсуждали? Что делает её уникальной?

(Ожидание ответа ученика)

Отлично. Кто может объяснить, что такое «информационный пузырь» и почему это явление может быть опасным? Сидорова, пожалуйста.

(Одиннадцатиклассница отвечает)

Хорошо. Теперь давайте вспомним основные манипулятивные технологии, которые используются в цифровой среде. Кузнецов, назови хотя бы три примера.

(Выслушивание школьника)

А сейчас я предлагаю вам небольшой практический тест. Посмотрите на экран. Перед вами три новостных сообщения. Используя изученные инструменты проверки достоверности информации, определите, какое из них может быть фейковым. На размышление — одна минута.

(Учащиеся анализируют задание)

Время вышло. Иванова, поделись своими наблюдениями. Какие признаки помогли тебе определить недостоверную информацию?

(Ожидание ответа ученицы)

И последний вопрос: какие практические навыки информационной безопасности вы уже начали применять в повседневной жизни? Кто готов поделиться своим опытом?

(Одиннадцатиклассники высказываются)

Прекрасно! Я вижу, что материал прошлого занятия вы усвоили хорошо. Эти знания станут прочным фундаментом для изучения новой темы, к которой мы сейчас перейдём.

Вступительное слово преподавателя-организатора

В современном мире каждый из нас проводит значительную часть жизни в цифровом пространстве. Мы общаемся в социальных сетях, совершаем покупки онлайн, пользуемся государственными услугами через интернет, учимся на онлайн-платформах. Но задумывались ли вы когда-нибудь о том, какие права имеет человек в цифровом мире? И главное – как их защищать?

Приведу простой пример. Вчера вечером кто-нибудь из вас делал селфи и выкладывал его в социальные сети?

(Ожидание реакции одиннадцатиклассников)

А знаете ли вы, что происходит с этой фотографией дальше? Кто имеет право её использовать? И что делать, если вы обнаружили, что ваше фото кто-то использует без вашего разрешения?

Или другая ситуация: вы заказали товар в интернет-магазине, но получили совсем не то, что хотели. Как защитить свои права в такой ситуации?

Сегодня тема нашего урока: «Защита прав в цифровом пространстве».

(Учитель записывает тему на доске)

На этом уроке мы с вами:

- разберём, какие права есть у человека в цифровой среде
- изучим основные угрозы этим правам
- научимся распознавать ситуации, когда наши свободы нарушаются
- и самое главное – освоим практические способы защиты своих действий в цифровом мире.

Это знание критически важно для каждого современного человека. Ведь, как говорится, предупреждён – значит вооружён. А в цифровом мире лучшая защита – это знание своих прав и умение их отстаивать.

> ***Цитата:***
> ***«Знания о том, как вести себя среди современных технологий — это не просто мудрость, а необходимость для каждого человека.»***
> ***— А.Н. Викторова, 1981–н.в., педагог и исследователь в области медиаграмотности.***

Готовы погрузиться в эту важную тему?

Основная часть

Иллюстративное фото / newUROKI.net

Права человека в цифровом пространстве

Основные цифровые права и свободы граждан РФ

Каждый человек имеет гарантированные законом возможности для безопасного использования технологий и защиты своих интересов в интернете.

Среди них:

- Конфиденциальность личной информации, которая запрещает третьим лицам без согласия собирать, обрабатывать или распространять сведения о человеке.
- Равенство доступа к цифровым ресурсам, независимо от социального статуса или убеждений.
- Свободное выражение мнения, что включает публикацию собственных взглядов в сети, если это не нарушает законов.
- Безопасное использование технологий, что обязывает разработчиков соблюдать стандарты, исключающие угрозы для пользователей.

Эти нормы регулируются как международными конвенциями, так и законами России, обеспечивая надежную основу для взаимодействия в цифровой среде.

Законодательные основы защиты прав в цифровой среде

В России действует ряд нормативных актов, направленных на охрану интересов пользователей. Основные из них:

- Федеральный закон «О персональных данных» регулирует порядок сбора и обработки личной информации.
- Закон «Об информации и информационных технологиях» устанавливает правила работы с контентом и меры противодействия киберугрозам.
- Гражданский кодекс защищает авторские права, включая цифровые разработки и произведения.
- Уголовный кодекс предусматривает наказания за мошенничество, хакерские атаки и другие преступления в сети.

Эти акты помогают эффективно защищать интересы граждан, а также предупреждать нарушения в области технологий.

Персональные данные и право на их защиту

> ***Персональные данные – это** любая информация, позволяющая идентифицировать конкретного человека. Примеры включают имя, адрес, телефонный номер, данные паспорта или банковского счёта.*

Определение

Эти сведения требуют особого подхода, поскольку:

- Могут быть использованы для мошенничества.
- Раскрытие личных данных без согласия нарушает права гражданина.

В России существует строгий порядок обработки таких сведений:

- Организации обязаны обеспечить их конфиденциальность.
- Каждый человек имеет возможность требовать удаления своих данных, если они используются незаконно.

Важно помнить, что безопасность начинается с действий самого пользователя: избегайте публикации лишних сведений в открытом доступе и будьте внимательны при заполнении онлайн-форм.

Право на доступ к информации и его ограничения

Все граждане имеют могут узнавать и использовать данные из доступных источников. Это помогает быть в курсе событий, законов и актуальных вопросов.

Однако существуют ограничения:

- Государственная тайна охраняется в целях безопасности страны.
- Частная жизнь других людей защищается законом.
- Запрещённый контент блокируется, чтобы не допустить пропаганды насилия, наркотиков или экстремизма.

Доступ к информации требует ответственности. Уважайте права других, проверяйте достоверность источников и соблюдайте правовые нормы.

Безопасность в цифровой среде

Иллюстративное фото / newUROKI.net

Виды угроз правам человека в цифровом пространстве

Современные технологии облегчают нашу жизнь, но также несут в себе потенциальные опасности.

Среди ключевых угроз:

- **Кража персональных данных:** злоумышленники могут получить доступ к конфиденциальной информации, такой как паспортные данные, номера банковских карт или адреса.
- **Мошенничество:** распространены фишинговые сайты, поддельные письма и предложения, которые обманом вынуждают пользователей передавать свои сведения или деньги.
- **Кибербуллинг:** агрессивное поведение в интернете, включая оскорбления и угрозы, способно нанести серьезный психологический вред.
- **Распространение вредоносных программ:** вирусы и шпионское ПО способны проникать в устройства, блокировать работу системы или похищать файлы.
- **Манипуляция сознанием:** использование недостоверной информации или алгоритмов для влияния на мнение и действия пользователей.

Стоит прочесть также: Правила дорожного движения - конспект урока

Инфографика / newUROKI.net

Эти угрозы требуют внимания и грамотного подхода для минимизации рисков.

Методы защиты личной информации

Чтобы защитить личные сведения, важно соблюдать несколько ключевых правил:

- **Сложные пароли:** создавайте уникальные комбинации из букв, цифр и символов для каждой учётной записи.
- **Двухфакторная аутентификация:** используйте дополнительный уровень защиты, например, одноразовые коды, отправляемые на телефон.
- **Обновление программного обеспечения:** своевременно устанавливайте обновления, которые устраняют уязвимости в системе.
- **Проверка ссылок и отправителей:** не переходите по подозрительным ссылкам, особенно из писем неизвестных адресатов.
- **Контроль настроек конфиденциальности:** ограничьте доступ к своим данным в социальных сетях и других приложениях.

Инфографика / newUROKI.net

Эти простые действия помогут предотвратить многие неприятные ситуации.

Правила безопасного поведения в социальных сетях

Социальные сети стали неотъемлемой частью жизни, но важно помнить о безопасности:

- Минимум личной информации: не публикуйте сведения, которые могут быть использованы против вас, такие как адрес или место работы.
- Настройка приватности: ограничьте круг лиц, которые видят ваши публикации.
- Осторожность в общении: не доверяйте незнакомцам и не раскрывайте им свои личные данные.
- Фильтрация контента: избегайте публикации материалов, которые могут нарушать законы или права других людей.
- Мониторинг своих действий: следите за своими комментариями и публикациями, чтобы не стать объектом критики или санкций.

Следование этим рекомендациям поможет сохранить вашу цифровую репутацию и безопасность.

Распознавание и противодействие мошенничеству в сети

Мошенники используют всё более изощрённые способы обмана.

Чтобы распознать их действия:

- **Будьте внимательны к предложениям «лёгкой наживы»:** слишком заманчивые предложения обычно скрывают подвох.
- **Проверяйте реквизиты:** перед оплатой товаров или услуг убедитесь, что сайт или продавец надежны.
- **Не переходите по подозрительным ссылкам:** часто фишинговые сайты маскируются под известные бренды.
- **Сохраняйте бдительность в электронных письмах:** мошенники часто отправляют письма от имени известных компаний, но с мелкими ошибками в адресе или тексте.

Если вы стали жертвой мошенников:

- Немедленно обратитесь в банк, если дело связано с денежными средствами.
- Сохраните доказательства: скриншоты сообщений, писем или сайтов.
- Сообщите в правоохранительные органы: напишите заявление о произошедшем.

Знание и применение этих рекомендаций поможет вам защитить себя и свои данные в интернете.

Ответственность за действия в интернете

Иллюстративное фото / newUROKI.net

Административная ответственность за правонарушения в сети

Деятельность пользователей в цифровом пространстве регулируется законами, которые устанавливают ответственность за несоблюдение норм и правил. Нарушения в интернете часто влекут за собой административные наказания, предусмотренные Кодексом Российской Федерации об административных правонарушениях.

Наиболее распространённые нарушения:

- **Оскорбление личности:** публичные высказывания, унижающие достоинство других пользователей. Наказание: штрафы, величина которых зависит от тяжести проступка.
- **Распространение ненадлежащей рекламы:** публикация материалов с ложной или вводящей в заблуждение информацией.
- **Нарушение порядка проведения митингов:** организация несогласованных акций или призывы к ним через интернет.
- **Использование нелегального контента:** публикация материалов, нарушающих общественные нормы или законодательство.

Инфографика / newUROKI.net

Административные санкции варьируются от предупреждений и штрафов до временной блокировки аккаунтов или сайтов.

Уголовная ответственность за преступления в цифровой среде

Некоторые нарушения в интернете классифицируются как преступления и подпадают под действие Уголовного кодекса РФ.

Это включает:

- **Мошенничество:** создание фальшивых сайтов, обман при интернет-торговле или хищение средств с банковских карт. Наказание: крупные штрафы, обязательные работы, лишение свободы.
- **Хакерские атаки:** несанкционированный доступ к компьютерным системам, кража конфиденциальной информации.
- **Разжигание ненависти или вражды:** публикации, направленные на дискриминацию по национальному, религиозному или другим признакам.
- **Пропаганда запрещённого контента:** распространение материалов экстремистского характера, детской порнографии или наркотических веществ.

Наказания за подобные деяния включают длительное лишение свободы, конфискацию имущества и другие меры, зависящие от тяжести преступления.

Ответственность за распространение недостоверной информации

В условиях цифровой эпохи распространение ложных сведений может нанести серьёзный ущерб обществу. Чтобы предотвратить это, законодательство РФ вводит санкции за дезинформацию.

Примеры действий, подпадающих под нарушение:

- **Фейковые новости:** публикация ложных сведений, способных вызвать панику или нанести вред репутации людей, организаций.
- **Искажение фактов:** преднамеренное манипулирование данными с целью ввести аудиторию в заблуждение.
- **Слухи, угрожающие безопасности:** создание или распространение информации, которая может нарушить общественный порядок.

За такие действия предусмотрены штрафы, блокировка контента и, в некоторых случаях, привлечение к уголовному наказанию.

Последствия нарушения авторских прав в интернете

Цифровое пространство облегчает доступ к интеллектуальной собственности, но это не отменяет необходимости соблюдать законы об авторских правах.

Использование произведений без разрешения владельца может привести к санкциям:

- **Незаконное скачивание или публикация:** фильмы, музыка, книги или программное обеспечение, выложенные без согласия правообладателя.
- **Плагиат***: выдача чужого труда за собственный, особенно в образовательных и научных работах.
- **Создание пиратских копий:** продажа или распространение материалов, защищённых законом, без лицензии.

> ***Плагиат — умышленно совершаемое физическим лицом незаконное использование или распоряжение охраняемыми результатами чужого творческого труда, которое сопровождается доведением до других лиц ложных сведений о себе как о действительном авторе.*** ***Википедия***

Наказания варьируются от предупреждений и штрафов до принудительных работ или тюремного заключения. Важно помнить, что наказание за использование нелицензионного контента лежит на каждом пользователе.

Таблица: Виды нарушений и возможные последствия

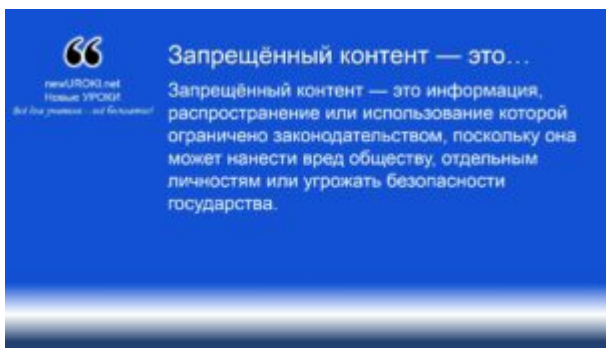
Нарушение	Последствия
Мошенничество	Уголовное наказание
Распространение ложной информации	Штраф или запрет на деятельность
Невозможность доступа к аккаунту	Потеря личных данных
Утечка приватных данных	Утрата репутации
Распространение вирусов	Потеря денежных средств

Запрещенный контент и правовые последствия

Иллюстративное фото / newUROKI.net

Классификация запрещённого контента

> ***Запрещённый контент — это** информация, распространение или использование которой ограничено законодательством, поскольку она может нанести вред обществу, отдельным личностям или угрожать безопасности государства.*



Определение

Примеры таких материалов:

- **Экстремистская информация:** призывы к насилию, разжигание вражды на национальной, религиозной или иной основе.
- **Порнографические материалы:** особенно те, которые содержат изображения с участием несовершеннолетних.
- **Пропаганда наркотиков:** описание методов их изготовления, употребления или рекламы.
- **Инструкции для незаконной деятельности:** пособия по созданию оружия, взрывчатых веществ, совершению преступлений.
- **Сведения, нарушающие права и свободы граждан:** такие как клевета или ложные сведения, направленные на подрыв репутации.

Каждая из этих категорий может нанести вред как отдельным людям, так и всему обществу, что делает её распространение незаконным.

Ответственность за создание и распространение

Создание и публикация сведений, признанных недопустимыми, является серьёзным нарушением закона. Ответственность за такие действия регулируется как административными, так и уголовными нормами.

Административная ответственность:

Штрафы за размещение нежелательной информации в открытом доступе.
Блокировка интернет-ресурсов, нарушающих законодательство.

Уголовная ответственность:

Лишение свободы за производство или продажу запрещённых материалов.
Привлечение к ответственности за публикации, угрожающие общественному порядку или государственной безопасности.
Помимо наказаний, нарушителям может быть запрещено занимать определённые должности, а также конфисковано оборудование, использованное для противоправной деятельности.

Алгоритм действий при обнаружении запрещённого контента

Если вы наткнулись на данные, которые могут быть признаны незаконными, важно следовать установленным правилам:

- **Не взаимодействовать с материалом:** не переходите по ссылкам, не скачивайте и не распространяйте его.
- **Сделать скриншот или сохранить ссылку:** эти данные могут понадобиться для обращения в компетентные органы.
- **Сообщить об обнаружении:** обратитесь в Роскомнадзор через официальный сайт или отправьте сообщение на горячую линию.
- **Сообщить правоохранительным органам:** в случае, если контент содержит признаки преступления (например, угрозы жизни или экстремизм).
- **Уведомить администрацию платформы:** если нежелательные сведения размещены в социальной сети, сообщите об этом модераторам.

Следование этим шагам помогает минимизировать риски и ускорить удаление опасных материалов.

Государственные системы блокировки нежелательного контента

Государство активно борется с распространением вредной информации, используя современные технологии и правовые механизмы.

Основные системы контроля:

- **Единый реестр запрещённых сайтов:** содержит ресурсы, которые были признаны недопустимыми. Доступ к ним блокируется операторами связи.
- **Системы фильтрации в образовательных учреждениях:** школы и университеты используют программное обеспечение для ограничения доступа к нежелательным ресурсам.
- **Сотрудничество с интернет-платформами:** такие компании, как Google и «ВКонтакте», обязаны удалять материалы по запросу государственных органов.
- **Интернет-мониторинг:** специальные службы, включая Роскомнадзор, отслеживают нарушения и принимают меры по блокировке сайтов.

Эти меры направлены на обеспечение безопасности граждан, защиту несовершеннолетних и снижение распространения вредной информации в интернете.

Механизмы защиты прав в цифровом пространстве

Иллюстративное фото / newUROKI.net

Государственные органы по защите прав в цифровой среде

В Российской Федерации действуют специализированные структуры, отвечающие за соблюдение законов в области информационной безопасности и взаимодействия в виртуальной среде.

- **Роскомнадзор:** выполняет функцию надзора за соблюдением законодательства в сфере информационных технологий, включая контроль за обработкой персональных данных и мониторинг запрещённого контента. Этот орган также управляет Единым реестром заблокированных сайтов.
- **Прокуратура:** рассматривает заявления граждан о нарушениях их интересов в электронном пространстве и принимает меры по привлечению виновных лиц к ответственности.
- **Полиция и подразделения по борьбе с киберпреступностью:** занимаются расследованием случаев мошенничества, взломов, кибербуллинга, а также других правонарушений, совершённых с использованием сети.
- **Суды общей юрисдикции:** рассматривают дела, связанные с нарушением интересов граждан в интернет-среде, в том числе вопросы, связанные с персональными данными, клеветой, взломами аккаунтов.

Эти структуры обеспечивают соблюдение законности и помогают людям защищать свои интересы при взаимодействии с интернетом.

Досудебное урегулирование споров

Во многих случаях споры, связанные с цифровыми нарушениями, можно разрешить до обращения в суд. Это позволяет сэкономить время, снизить затраты и урегулировать конфликт без привлечения сторонних органов.

Процедура досудебного разрешения:

- **Обращение к нарушителю:** Если ваши интересы нарушены, например, кто-то неправомерно использует вашу фотографию или распространяет ложную информацию, первым шагом станет обращение к этому лицу с просьбой удалить материал или прекратить действия.
- **Жалоба в администрацию платформы:** Социальные сети, видеохостинги и другие интернет-ресурсы предоставляют специальные инструменты для подачи жалоб. Например, вы можете отметить публикацию как нежелательную, отправить запрос на блокировку или связаться с модераторами.
- **Обращение в Роскомнадзор:** Если проблема остаётся нерешённой, вы можете подать жалобу в этот орган. Роскомнадзор рассматривает такие заявления и может предпринять меры, включая блокировку ресурса.

- **Медиация:** В сложных случаях возможно привлечение медиаторов — специалистов, которые помогают сторонам конфликта прийти к соглашению без судебного разбирательства.

Досудебное урегулирование помогает избежать длительных процедур и зачастую позволяет оперативно устранить причины.

Судебная защита нарушенных прав

Если конфликт не удалось разрешить мирным путём, гражданин вправе обратиться в суд. Судебное разбирательство является одной из основных гарантий восстановления справедливости.

- **Исковые требования:** В заявлении указываются суть правонарушения, доказательства и требования к ответчику, например, компенсация морального ущерба или удаление незаконного материала.
- **Доказательная база:** Для успешного рассмотрения дела важно предоставить скриншоты, ссылки, переписку и другие материалы, подтверждающие факт нарушения.
- **Судебное решение:** После рассмотрения дела суд выносит постановление, обязательное для исполнения. Это может быть штраф, блокировка ресурса или возмещение убытков.

Стоит прочесть также: [Профилактика и первая помощь при отравлениях - конспект урока]

Суды также могут принимать временные меры, такие как блокировка доступа к информации на период разбирательства.

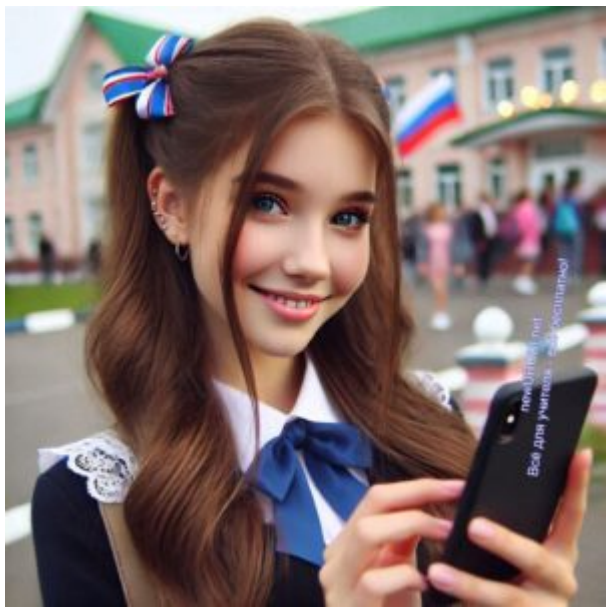
Роль общественных организаций в защите цифровых прав

Немалую роль в обеспечении безопасности в интернете играют общественные и правозащитные организации. Они занимаются поддержкой людей, популяризацией знаний и контролем за действиями государственных органов.

- **Фонды защиты:** предоставляют бесплатные консультации, юридическую помощь и образовательные программы для пользователей интернета.
- **Общественные инициативы:** такие проекты, как «Безопасный интернет», занимаются просветительской работой, обучают правилам безопасности в сети и предлагают ресурсы для защиты личных данных.
- **Профсоюзы и ассоциации:** объединения журналистов, блогеров и других участников цифровой среды защищают их интересы, особенно в ситуациях, связанных с цензурой или нарушением свободы слова.

Эти структуры активно взаимодействуют с государственными органами, участвуют в разработке законов и помогают гражданам в сложных ситуациях.

Практические навыки защиты прав



Иллюстративное фото / newUROKI.net

Настройка конфиденциальности в социальных сетях

В современном мире социальные сети стали частью повседневной жизни. Однако неправильная настройка конфиденциальности может привести к утечке личной информации.

Чтобы избежать этого, следует:

- **Ограничить видимость профиля:** В настройках учетной записи можно сделать профиль закрытым, чтобы его могли видеть только одобренные вами пользователи.
- **Контроль публикаций:** Установите ограничения на просмотр ваших постов и фотографий для определённых групп пользователей. Например, сделайте публикации доступными только для друзей.
- **Проверить подключённые приложения:** Отключите сторонние программы, которые имеют доступ к вашей странице, если они вам больше не нужны.
- **Двухфакторная аутентификация:** Этот метод добавляет дополнительный уровень безопасности — помимо пароля, потребуется подтверждение через SMS или приложение.
- **Регулярное обновление пароля:** Используйте сложные комбинации символов и меняйте пароль каждые несколько месяцев.

Эти простые действия помогут сохранить вашу информацию в безопасности и предотвратить её несанкционированное использование.

Алгоритм действий при нарушении цифровых прав

Если ваши интересы в интернете были ущемлены, важно действовать быстро и грамотно:

- **Соберите доказательства:** Сделайте скриншоты, сохраните переписку, ссылки и другие материалы, подтверждающие факт нарушения.
- **Обратитесь к виновнику:** Если это возможно, свяжитесь с лицом или организацией, причинившими вред, с требованием прекратить противоправные действия.
- **Жалоба в администрацию сайта:** Используйте встроенные инструменты жалоб для удаления нежелательного контента или блокировки аккаунта нарушителя.
- **Заявление в уполномоченные органы:** Если проблема не решена, подайте жалобу в Роскомнадзор, полицию или прокуратуру. В заявлении укажите все детали инцидента и приложите доказательства.
- **Юридическая помощь:** При сложных ситуациях рекомендуется обратиться за консультацией к юристам, специализирующимся на цифровой защите.

Чёткое соблюдение этих шагов поможет вам восстановить справедливость и привлечь нарушителей к ответственности.

Составление обращений в уполномоченные органы

При нарушении ваших интересов в интернете важно правильно оформить заявление:

- **Форма обращения:** Обращение можно подать в электронном виде через сайты государственных органов (например, Роскомнадзора) или в бумажной форме лично или по почте.
- **Содержание:** Укажите ваши данные (ФИО, адрес, контактный телефон), подробно опишите суть проблемы, добавьте доказательства и сформулируйте требования. Например, это может быть просьба удалить клеветнический материал, заблокировать аккаунт мошенника или пресечь незаконные действия.
- **Сроки рассмотрения:** По закону обращение должно быть рассмотрено в течение 30 дней, однако в экстренных случаях этот срок может быть сокращён.
- **Ответ:** Вы получите уведомление о принятых мерах. Если вас не устроит результат, вы можете подать жалобу в вышестоящую инстанцию или в суд.

Корректно составленное заявление значительно повышает вероятность успешного разрешения ситуации.

Использование технических средств защиты информации

Технические инструменты играют ключевую роль в обеспечении безопасности в интернете.

Среди самых эффективных:

- **Антивирусные программы:** Защищают устройства от вредоносного ПО, которое может похитить личные данные или нанести вред.
- **VPN-сервисы:** Скрывают ваше местоположение и защищают данные, передаваемые через интернет, особенно при использовании общедоступных Wi-Fi-сетей.
- **Менеджеры паролей:** Хранят сложные пароли и генерируют уникальные комбинации для каждого сайта, что предотвращает взлом.
- **Файрволы:** Блокируют несанкционированный доступ к вашему устройству через интернет.
- **Шифрование данных:** Используется для защиты информации на устройствах и при её передаче, что делает её недоступной для третьих лиц.

Используя эти технологии, вы сможете минимизировать риски и обеспечить высокий уровень безопасности в цифровой среде.

Рефлексия

Итак, друзья, пришло время для того, чтобы провести рефлексию и немного задуматься о том, что мы сегодня узнали. Давайте вместе оценим, насколько важно то, о чём мы говорили на занятии, и как это может повлиять на ваше повседневное поведение в интернете.

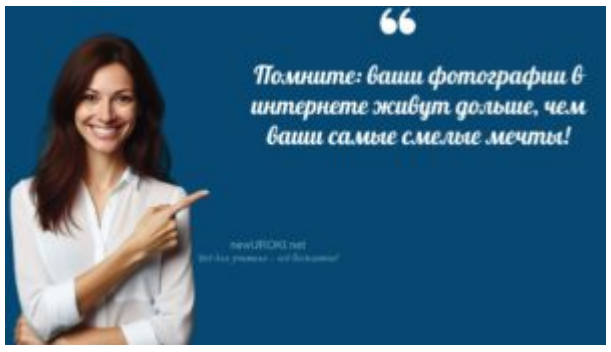
Попробуйте ответить на несколько вопросов для себя:

- Что нового я узнал(а) о том, как защищать свои данные в интернете?
- Какие моменты на занятии показались мне наиболее важными или интересными?
- Чувствую ли я себя более уверенно, зная, какие шаги нужно предпринять для своей безопасности в сети?
- Были ли моменты, которые вызвали у меня сомнения или вопросы? Что нужно уточнить или изучить дополнительно?

Сейчас мы сделаем паузу и попробуем подумать, как полученные знания могут повлиять на наше поведение в интернете. Как вы думаете, как эти рекомендации можно применять на практике? Что бы вы порекомендовали своим друзьям или родственникам, чтобы помочь им обезопасить себя в сети?

Поделитесь, кто хочет, своими размышлениями или вопросами, которые возникли в процессе. Это поможет нам понять, что стало для вас наиболее важным.

Заключение



Учителя шутят

Сегодняшнее занятие дало вам возможность взглянуть на важнейшие аспекты взаимодействия с цифровым миром и его влияния на вашу личную безопасность. Помните, что вы не просто пользователи сети — вы её активные участники, и ваша осведомленность помогает вам не только защищать себя, но и поддерживать доверительную атмосферу в интернете.

Теперь, когда у вас есть знания о том, как действовать в ситуациях, связанных с угрозами в виртуальном пространстве, вы можете уверенно двигаться вперёд. Ведь главное — это не только защищаться, но и понимать, как правильно пользоваться всеми инструментами, которые находятся у вас под рукой.

Каждый из вас способен сделать свою цифровую жизнь более безопасной, а значит, и более комфортной. Помните, что ваши действия имеют значение не только для вас, но и для окружающих. Применяйте знания, будьте внимательны и не забывайте о своих возможностях!

Верьте в себя, и вы сможете эффективно противостоять любым вызовам, которые встречаются на вашем пути в цифровом пространстве. Ваша безопасность — в ваших руках, и с каждым новым шагом вы становитесь всё более уверенными в своей способности защищать свои интересы и данные.

Домашнее задание

Ученики шутят

Обязательная часть:

- Изучить § параграф учебника
- Составить памятку «Мои действия при обнаружении нарушения моих прав в цифровой среде» (краткий алгоритм из 5-7 пунктов)

Дополнительно (по желанию):

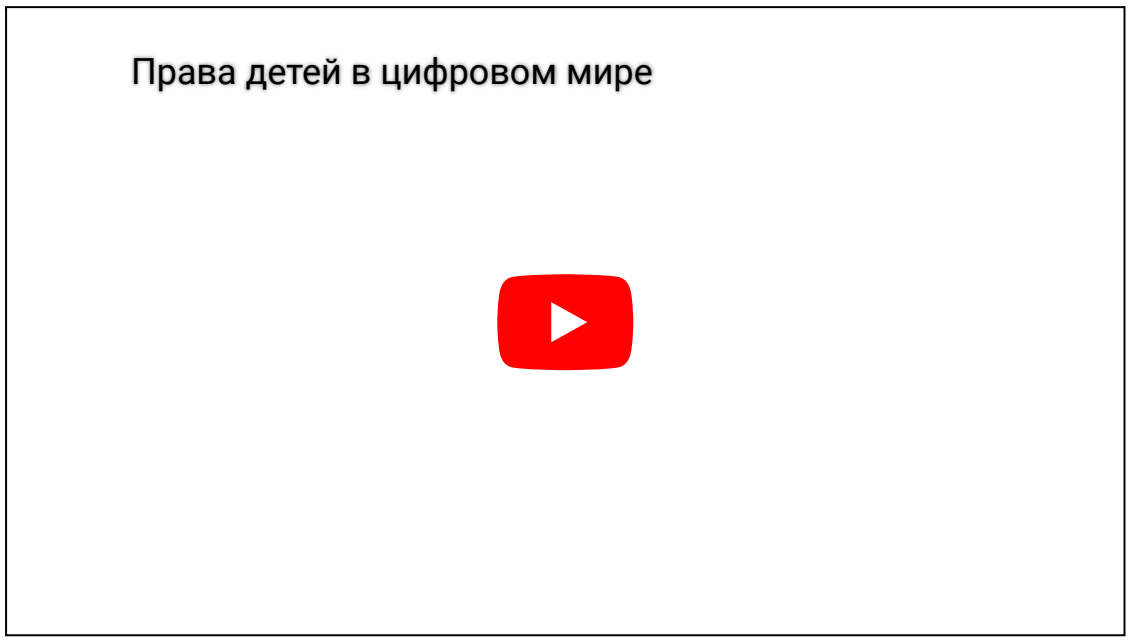
- Подготовить сообщение об одном из реальных случаев успешной защиты прав граждан в цифровом пространстве
- Провести анализ настроек конфиденциальности в своих социальных сетях и составить список необходимых изменений для повышения безопасности

Технологическая карта

Скачать бесплатно технологическую карту урока по теме: «Защита прав в цифровом пространстве»

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: «Защита прав в цифровом пространстве» в формате Ворд

Чек-лист педагога

Скачать бесплатно чек-лист для проведения урока ОБЗР по теме: «Защита прав в цифровом пространстве» в формате Word

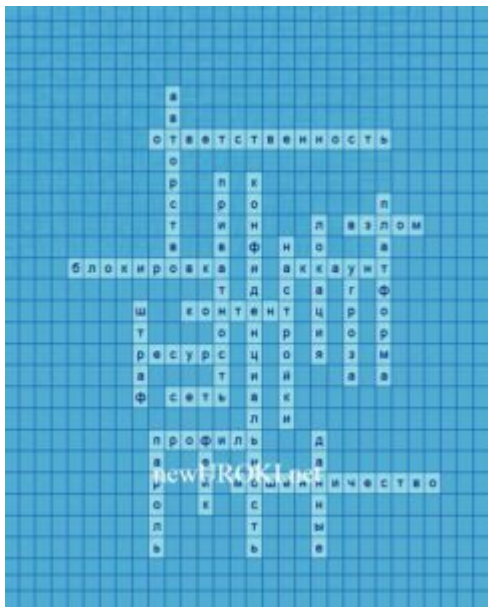
Чек-лист для учителя — это инструмент педагогической поддержки, представляющий собой структурированный перечень задач, шагов и критериев, необходимых для успешного планирования, подготовки и проведения урока или мероприятия.

Карта памяти для учеников

Скачать бесплатно карту памяти для учеников 11 класса по ОБЗР по теме: «Защита прав в цифровом пространстве» 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: «Защита прав в цифровом пространстве» в формате WORD]

Тесты

При регистрации в онлайн-сервисе безопаснее всего:
a) Указывать минимум личных сведений
b) Давать максимально подробную анкету
c) Рассказывать о своих предпочтениях
Правильный ответ: a

Самым надежным способом сохранения конфиденциальности является:
a) Использование одного пароля везде
b) Комбинация букв, цифр и символов в паролях
c) Запись паролей в блокнот
Правильный ответ: b

При обнаружении мошенничества следует:
a) Написать гневный комментарий
b) Проигнорировать ситуацию
c) Обратиться в соответствующие органы
Правильный ответ: c

Безопасное поведение в соцсетях включает:
a) Открытый доступ к фотографиям
b) Настройку ограничений доступа
c) Публикацию личных документов
Правильный ответ: b

При совершении покупок в сети необходимо:
a) Сообщать код с обратной стороны карты
b) Проверять надежность продавца
c) Переводить деньги без чека
Правильный ответ: b

Для безопасного общения рекомендуется:
a) Делиться личными данными
b) Встречаться с незнакомцами
c) Ограничивать круг контактов
Правильный ответ: c

При получении подозрительного сообщения следует:
a) Удалить его без перехода по ссылкам
b) Переслать всем друзьям

c) Открыть все вложения
Правильный ответ: a

Безопасное использование Wi-Fi предполагает:
a) Подключение к любой сети
b) Использование только надежных сетей
c) Передачу важных данных через открытые сети
Правильный ответ: b

При возникновении спорной ситуации с онлайн-магазином нужно:
a) Удалить историю заказа
b) Сохранить всю переписку и чеки
c) Создать новый аккаунт
Правильный ответ: b

Для сохранения личных данных важно:
a) Делать резервные копии
b) Хранить всё в одном месте
c) Давать доступ всем
Правильный ответ: a

Интересные факты для занятия

1. **Интересный факт 1:**
   В 2023 году средний подросток тратит около 7 часов в день на соцсети и мессенджеры, что сопоставимо с полноценным рабочим днём. При этом 85% молодых людей не проверяют надёжность сайтов перед вводом личных данных, делая себя уязвимыми для злоумышленников.
2. **Интересный факт 2:**
   Современные технологии распознавания лиц настолько совершенны, что могут идентифицировать человека даже по фрагменту фотографии, где видно всего 10% лица. Поэтому каждое селфи в открытом доступе может быть использовано для создания фейковых аккаунтов или даже deepfake-видео.
3. **Интересный факт 3:**
   Исследователи из Стэнфордского университета выяснили, что злоумышленники тратят в среднем всего 4 минуты на взлом аккаунта с простым паролем. В то же время для подбора сложного пароля, состоящего из 12 символов (включая буквы разного регистра, цифры и специальные знаки), потребуется около 34 тысяч лет даже при использовании мощных компьютеров.

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

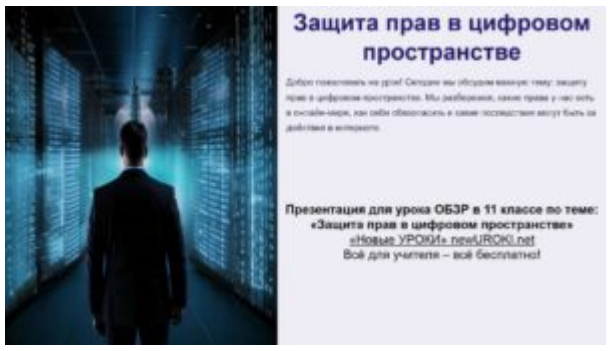
материал.

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: «Защита прав в цифровом пространстве» в формате PowerPoint

БОНУС: Рабочий лист

Скачать бесплатно рабочий лист по ОБЗР по теме: «Защита прав в цифровом пространстве» 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. Ханукович Н.С., «Основы безопасности в обществе». Издательство «Сириус», Санкт-Петербург, 2004. 250 страниц.
2. Околелов В.П., «Угрозы и риски в современной среде». Издательство «Лидер плюс», Москва, 2002. 210 страниц.
3. Укельман И.И., «Нормы и стандарты в обеспечении личной безопасности». Издательство «Сфера», Нижний Новгород, 2005. 190 страниц.
4. Алексеева Т.А., «Влияние современных технологий на общество». Издательство «ШАНС», Екатеринбург, 2001. 230 страниц.
5. Звонцова О.В., «Современные методы предотвращения нарушений в виртуальной среде». Издательство «Курс-принт», Ростов-на-Дону, 2003. 170 страниц.

0 НРАВИТСЯ 0 НЕ НРАВИТСЯ

50% Нравится Или 50% Не нравится

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

Расскажите о нас!

Слова ассоциации (тезаурус) к уроку: конфиденциальность, мошенничество, угрозы, доступ, аккаунт, блокировка, нарушения, платформа, ресурсы, приватность.

Достоверность информации — конспект урока »

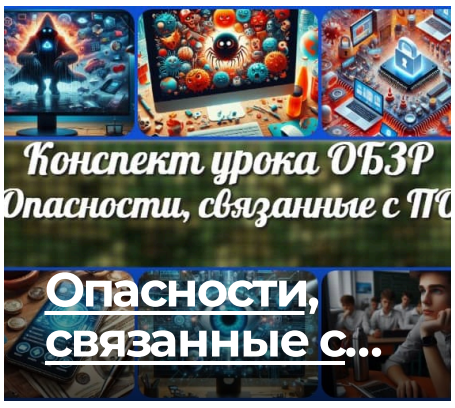
Автор Глеб Беломедведев

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

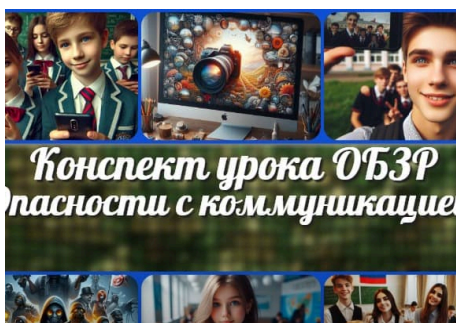
Достоверность информац...

Опасности с коммуникац...



Опасности, связанные с...

ИНТЕРЕСНЫЕ КОНСПЕКТЫ УРОКОВ



Новые УРОКИ

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

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