9 КЛАСС ОБЗР

Вредоносные программы — конспект урока

Автор Глеб Беломедведев

ФЕВ 3, 2025 20 фото Время прочтения: 38 минут(ы)

Просмотров: 7

#видео, #вирус, #вред, #защита, #интеллект-карта, #интересные факты, #карта памяти, #классификация, #кроссворд, #ментальная карта, #навык, #навыки, #облако слов, #полезные советы, #презентация, #признаки, #рабочий лист, #система, #среда, #таблица, #тесты, #технологическая карта, #цифровая, #чек-лист, #черви

Содержание [Скрыть]

1 Вредоносные программы и приложения, способы защиты от них. Опасные программы и явления цифровой среды — 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
Английский язык
Астрономия
10 класс
Библиотека
Биология
5 класс
6 класс
7 класс
8 класс
География
5 класс
6 класс
7 класс
8 класс
9 класс
10 класс
Геометрия
Директору и завучу школы
Должностные инструкции
ИЗО
Информатика
История

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 учителя
23 Основная часть
23.1 Понятие и классификация вредоносных программ
23.2 Признаки заражения устройства вредоносными программами
23.3 Методы защиты от вредоносных программ
23.4 Правила кибергигиены в цифровой среде
23.5 Опасные явления в социальных сетях и мессенджерах
23.6 Практические навыки защиты в цифровой среде
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

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

Вредоносные программы и приложения, способы защиты от них. Опасные программы и явления цифровой среды — конспект урока ОБЗР (Основы безопасности и защиты Родины)

Вступление

> ***В современном мире каждый подросток проводит в цифровом пространстве несколько часов ежедневно. Однако не все знают, что их смартфон может стать невольным предателем, раскрыв злоумышленникам личные данные или банковские реквизиты родителей. В этом конспекте вы найдете не только актуальную информацию о цифровых угрозах, но и практические материалы для проведения увлекательного мероприятия: технологическую карту, бесплатную презентацию, тематический кроссворд, тесты и рабочие листы для девятиклассников.***

Выберите похожие названия

- Методическая разработка: «Киберугрозы современного мира и методы противодействия им»
- Интерактивное занятие: «Цифровая безопасность подростка в современном мире»
- Практикум: «Основы информационной гигиены и защиты личных данных»
- 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 мультимедийных технологий

Цель

- Формирование у обучающихся знаний о вредоносных программах и навыков безопасного поведения в цифровой среде

Задачи

- **Обучающая:** сформировать представление о видах вредоносных приложений и способах защиты от них
- **Развивающая:** развить навыки критического мышления при работе в цифровой среде
- **Воспитательная:** воспитать ответственное отношение к информационной защищённости

Универсальные учебные действия (УУД)

- **Личностные УУД:** формирование ответственного отношения к собственной информационной защите
- **Регулятивные УУД:** развитие умения планировать свои действия в цифровой среде
- **Познавательные УУД:** освоение способов защиты от вредоносных программ
- **Коммуникативные УУД:** развитие умения взаимодействовать в группе при решении учебных задач
- **Метапредметные УУД:** формирование навыков безопасного использования цифровых устройств

Методические приёмы, педагогические методы, технологии обучения

- Мозговой штурм
- Интерактивный опрос
- Практическая работа с тестовыми заданиями
- Работа в малых группах
- Создание ментальной карты

Ожидаемые результаты

- **Личностные:** формирование ответственного отношения к защищённости в цифровой среде
- **Метапредметные:** развитие умения анализировать информацию и принимать решения в нестандартных ситуациях

- **Предметные:** знание основных видов вредоносных приложений и способов защиты от них

Предварительная работа педагога

- Подготовка презентации
- Разработка кроссворда, технологической карты
- Составление рабочих листов, тестовых заданий
- Подготовка карточек с кейсами для групповой работы
- Поиск видеоуроков и видеороликов
- Создание интеллект-карты, облака слов

Оборудование и оформление кабинета

- Компьютер с проектором
- Интерактивная доска
- Раздаточный материал (рабочие листы)
- Карточки с заданиями для групповой работы
- Плакаты

Ход занятия / Ход мероприятия

Организационный момент

Здравствуйте, ребята! Прошу всех занять свои места. Дежурные, пожалуйста, подготовьте проекционный экран к работе.

Давайте проведём перекличку…

(проводится перекличка по списку)

Так, теперь проверим готовность к занятию. У каждого на парте должны быть: тетрадь для записей, ручка, карандаш и учебник. Проверьте, пожалуйста… Вижу, что все подготовились, молодцы!

Обратите внимание на свой внешний вид — рукава должны быть опущены, спина прямая, сидим ровно. Это важно для вашего здоровья и правильной посадки за партой.

Напоминаю правила поведения: когда отвечаете — поднимаем руку, не перебиваем друг друга, уважаем мнение одноклассников. И очень важный момент — пожалуйста, отключите звук на ваших мобильных телефонах, они нам сегодня не понадобятся для работы.

Я вижу, что сегодня у нас замечательная погода за окном, и у всех прекрасное настроение! Это здорово, потому что нам предстоит очень интересное и познавательное мероприятие. Я уверен, что каждый из вас узнает что-то новое и полезное для себя.

Перед тем как мы начнем, давайте улыбнемся соседу по парте — ведь позитивный настрой очень важен для успешной работы. Вот так, отлично! Теперь мы точно готовы к продуктивному занятию!

Актуализация усвоенных знаний

Дорогие девятиклассники, на прошлом занятии мы с вами подробно рассматривали тему: «Цифровая среда — ее возможности и риски. Общие принципы безопасности в цифровой среде» . Давайте проверим, как хорошо вы усвоили этот материал. Я буду задавать вопросы, а вы поднимайте руку, если готовы ответить.

Вспомните, пожалуйста, что такое цифровая среда? Кто может дать определение?

(ожидание ответов школьников)

Отлично! А теперь давайте подумаем о положительных сторонах интернет-среды. Какие возможности она нам даёт? Предлагаю каждому назвать по одному преимуществу. Начнём с первого ряда…

(выслушивание ответов)

Хорошо, но ведь мы говорили и об угрозах. Кто может назвать основные риски использования интернета?

(ожидание ответов)

А сейчас я хочу, чтобы вы вспомнили принципы безопасного поведения в цифровой среде. Запишем их на доске. Я буду записывать, а вы предлагайте…

(запись на доске предложенных учениками принципов)

И последний вопрос: какие меры безопасности вы уже применяете в своём личном цифровом пространстве? Поделитесь своим опытом…

(обсуждение практического опыта учащихся)

Я вижу, что материал прошлого занятия вы усвоили хорошо. Эти знания нам очень пригодятся сегодня, потому что мы будем углубляться в тему цифровой безопасности и рассмотрим её более детально.

Вступительное слово учителя

Друзья, мы с вами живём в удивительное время, когда практически у каждого из нас есть мощный компьютер в кармане — наш смартфон. С его помощью мы общаемся с друзьями, учимся, развлекаемся. Но задумывались ли вы когда-нибудь, что ваш надёжный цифровой помощник может стать источником серьёзных проблем?

Представьте ситуацию: вы скачали новую игру или приложение, а через некоторое время обнаружили, что ваши личные фотографии или переписка оказались в открытом доступе. Или ещё хуже — с банковской карты родителей начали списываться деньги. Как такое возможно?

Сегодня мы с вами поговорим об очень важной теме. На этом занятии вы узнаете, какие опасности могут скрываться в, казалось бы, безобидных программах, и главное — как от них защититься.

Запишите, пожалуйста, тему урока в тетрадь: «Вредоносные программы и приложения, способы защиты от них»

(Пауза для записи)

Мы разберём основные виды вредоносных программ, научимся распознавать признаки заражения устройства и, самое главное, освоим эффективные методы защиты от цифровых угроз. Эти знания помогут вам сохранить в безопасности не только свои данные, но и защитить своих близких от киберпреступников.

> ***Цитата:***
> ***«Если бы люди охраняли свои онлайн-аккаунты так же, как двери своего дома, интернет был бы гораздо безопаснее»***
> ***— Д.В. Колосов, 1975–н.в., российский программист, эксперт по киберугрозам.***

Готовы погрузиться в мир цифровой безопасности? Тогда начнём!

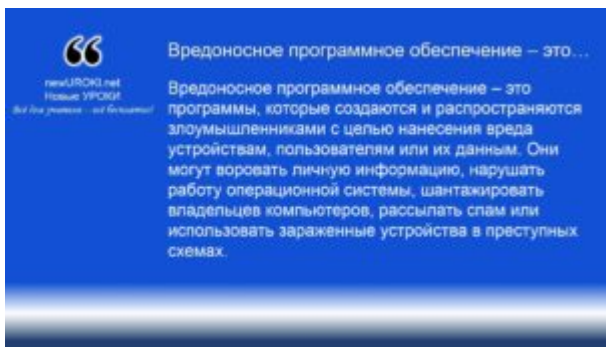
Основная часть

Иллюстративное фото / newUROKI.net

Понятие и классификация вредоносных программ

Определение

> ***Вредоносное программное обеспечение – это** программы, которые создаются и распространяются злоумышленниками с целью нанесения вреда устройствам, пользователям или их данным. Они могут воровать личную информацию, нарушать работу операционной системы, шантажировать владельцев компьютеров, рассылать спам или использовать зараженные устройства в преступных схемах.*

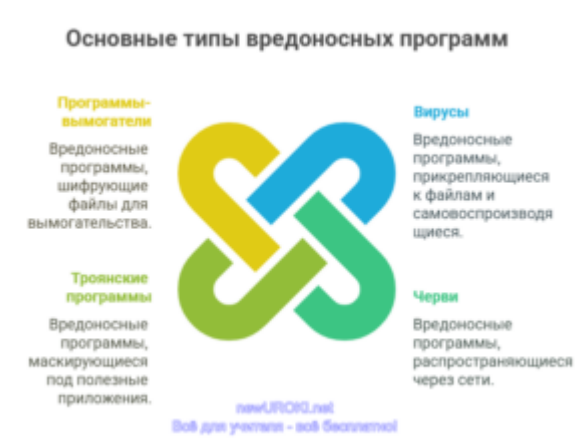


Определение

Основные типы вредоносных программ

Существует несколько основных видов вирусного программного обеспечения:

- **Компьютерные вирусы** – они прикрепляются к файлам и приложениям, активируются при их запуске и могут самовоспроизводиться. Вирусы способны уничтожать файлы, изменять данные и нарушать работу системы.
- **Черви** – вредоносные утилиты, которые распространяются без участия пользователя. Они в состоянии перемещаться через сети и заражать другие устройства, используя уязвимости операционной системы.
- **Троянские программы (трояны)** – маскируются под полезные приложения, но при установке выполняют вирусные действия, например, открывают доступ к устройству для злоумышленников или воруют данные.
- **Программы-вымогатели (шифровальщики, ransomware)** – блокируют доступ к устройству или шифруют файлы, требуя от пользователя деньги за их восстановление.



Инфографика / newUROKI.net

Помимо этих основных типов, существуют также рекламное ПО (adware), шпионское ПО (spyware), кейлоггеры (утилиты для перехвата нажатий клавиш) и ботнеты (приложения, позволяющие хакерам управлять зараженными компьютерами).

Способы распространения вредоносных программ

Злоумышленники используют разные методы для распространения вредоносного ПО.

Основные способы заражения устройств:

- Файлы из ненадежных источников – вирусы могут быть скрыты в программах, которые скачиваются с подозрительных сайтов или пиратских ресурсов.
- Электронные письма и вложения – фишинговые письма часто содержат вложенные файлы или ссылки на вредоносные сайты.
- Социальные сети и мессенджеры – ссылки на зловредные приложения рассылаются через сообщения от взломанных аккаунтов.
- Флешки и внешние носители – зараженные флеш-накопители могут автоматически запускать вирусные утилиты при подключении к компьютеру.
- Рекламные баннеры и всплывающие окна – клики по таким баннерам могут привести к загрузке вируса.
- Фальшивые обновления – злоумышленники очень часто предлагают скачать «обновление» для браузера или антивируса, но на самом деле это вирус.
- Использование уязвимостей в ПО – вирусы способны проникать на устройства через дыры в безопасности операционных систем и сторонних приложений.

Вредоносные программы представляют серьезную угрозу, но грамотное использование антивирусного ПО, осторожность при скачивании файлов и внимательность в сети помогают избежать заражения.

Признаки заражения устройства вредоносными программами

Иллюстративное фото / newUROKI.net

Современные киберугрозы могут незаметно проникнуть на компьютер, смартфон или планшет, нанося ущерб системе и передавая данные злоумышленникам. Однако существуют явные признаки, которые помогут своевременно обнаружить наличие

нежелательного ПО и принять меры.

Изменения в работе устройства

Одним из первых сигналов проникновения вирусного кода являются различные сбои и нестабильность системы.

Например:

- **Замедление работы.** Даже мощные устройства неожиданно начинают зависать, тормозить, долго загружаться или медленно реагировать на команды. Это может быть связано с тем, что в фоновом режиме работает зловредное ПО, потребляющее ресурсы процессора и оперативной памяти.
- **Неожиданные перезагрузки.** Если компьютер или смартфон перезагружается без видимой причины, это очень часто указывает на вмешательство вредоносного кода, особенно если сбои происходят регулярно.
- **Ошибки при запуске программ.** Если привычные приложения начинают закрываться с сообщением об ошибке или вовсе не запускаются, это может быть результатом работы вируса, который изменяет системные файлы.
- **Поврежденные или пропавшие данные.** Если некоторые файлы внезапно исчезли или стали нечитаемыми, существует вероятность, что на устройство проник шифровальщик, блокирующий доступ к данным.

Инфографика / newUROKI.net

Подозрительная сетевая активность

Некоторые вредоносные коды активно взаимодействуют с интернетом, отправляя информацию злоумышленникам или загружая дополнительные файлы.

В таких случаях могут наблюдаться следующие симптомы:

- **Неожиданное увеличение интернет-трафика.** Если пользователь не скачивал больших файлов, но соединение стало медленным, возможно, вирус использует интернет-канал для передачи данных.
- **Автоматическое открытие браузера и сторонних сайтов.** Внезапное появление незнакомых страниц при запуске браузера или постоянные перенаправления на подозрительные ресурсы указывают на заражение.
- **Неизвестные процессы в диспетчере задач.** Если среди запущенных процессов в системе появились незнакомые или аномально загружающие процессор, это способно быть признаком активности трояна или бота.
- **Подозрительные входящие и исходящие сообщения.** Вирусные скрипты часто рассылают спам от имени пользователя, отправляют мошеннические ссылки его контактам или используют почтовый клиент для распространения заражённых вложений.

Стоит прочесть также: Культура безопасности - конспект урока

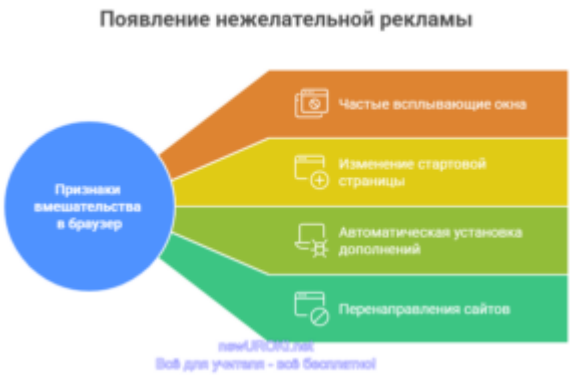
Инфографика / newUROKI.net

Появление нежелательной рекламы и всплывающих окон

Некоторые вирусы связаны с рекламной деятельностью, захватывая контроль над браузером и отображая назойливые объявления.

Проявляется это следующим образом:

- **Частые всплывающие окна.** При работе в браузере или даже в системных приложениях могут появляться нежелательные рекламные баннеры, предложения скачать сомнительное ПО или уведомления о «выигрыше» в лотерее.
- **Изменение стартовой страницы браузера.** Если домашняя страница самопроизвольно сменилась, а при попытке ее изменить — изменения не сохраняются, это, вероятно, следствие воздействия вредоносного расширения.
- **Автоматическая установка неизвестных дополнений.** В браузере могут появляться лишние панели инструментов, расширения или плагины, которых пользователь не устанавливал.
- **Перенаправления при вводе адресов.** Если при попытке открыть один сайт происходит переадресация на другой ресурс с сомнительным содержимым, это явный сигнал о наличии угрозы.



Инфографика / newUROKI.net

Обнаружив хотя бы один из перечисленных признаков, необходимо немедленно проверить устройство с помощью антивирусного ПО и удалить все подозрительные файлы. Кроме того, рекомендуется отключить интернет-соединение, чтобы предотвратить дальнейшую передачу данных злоумышленникам.

Методы защиты от вредоносных программ

Иллюстративное фото / newUROKI.net

Современная цифровая среда таит множество угроз, способных нанести вред устройствам и конфиденциальным данным пользователей. Чтобы минимизировать риски и обеспечить безопасность личной информации, необходимо соблюдать комплекс мер, направленных на предотвращение заражения и устранение возможных атак.

Установка и обновление антивирусного программного обеспечения

Одним из основных способов предохранения от киберугроз является использование антивирусных решений. Эти системы выявляют и нейтрализуют потенциально опасные объекты, обеспечивая надежный контроль за состоянием операционной системы.

- **Выбор защитного ПО.** Существует множество антивирусных приложений, отличающихся функциональностью и уровнем защиты. Важно выбирать проверенные решения от известных разработчиков, регулярно получающие обновления и обладающие хорошей репутацией среди пользователей.
- **Обновление баз сигнатур.** Киберпреступники постоянно разрабатывают новые схемы атак, поэтому разработчики антивирусов регулярно обновляют базы данных, добавляя в них сведения о последних угрозах. Если вовремя не обновлять сигнатуры, защита теряет свою актуальность, и устройство становится уязвимым.
- **Проверка компьютера.** Желательно регулярно сканировать устройство на предмет подозрительных объектов. Даже если антивирус работает в фоновом режиме, он может пропустить скрытые угрозы, поэтому рекомендуется запускать полное сканирование хотя бы раз в неделю.
- **Функция проактивной защиты*.** Современные антивирусные решения обладают функциями поведенческого анализа, которые помогают выявлять неизвестные вредоносные компоненты, ориентируясь на их активность. Включение такого режима позволяет блокировать потенциальные угрозы еще до их попадания в базу антивируса.

> ***Проактивные технологии** — совокупность технологий и методов, используемых в антивирусном программном обеспечении, основной целью которых, в отличие от реактивных технологий, является предотвращение заражения системы пользователя, а не поиск уже известного вредоносного программного обеспечения в системе. Википедия*

Настройка брандмауэра и параметров безопасности

Дополнительной линией обороны служит системный экран (брандмауэр), который контролирует входящий и исходящий трафик, предотвращая несанкционированный доступ к устройству.

- **Активация встроенного сетевого экрана.** Большинство операционных систем оснащены встроенными брандмауэрами, которые необходимо активировать. Они фильтруют входящие соединения, блокируя подозрительную активность со стороны внешних сетей.
- **Ограничение сетевых подключений.** Некоторые приложения запрашивают доступ к интернету без необходимости. В настройках безопасности можно ограничить сетевую активность для ненадежных программ, предотвратив возможную передачу информации третьим лицам.
- **Использование фильтров веб-контента.** Вредоносные файлы часто распространяются через сомнительные сайты. Настройка защиты интернет-браузера и использование специальных плагинов, блокирующих переход на опасные ресурсы, помогают снизить вероятность заражения.
- **Контроль обновлений операционной системы.** Разработчики ПО регулярно выпускают исправления уязвимостей, обнаруженных в программном коде. Автоматическое обновление системы позволяет своевременно устранять слабые места в защите.

Регулярное резервное копирование данных

Даже при строгом соблюдении всех мер предосторожности существует риск потери информации из-за атак вымогателей или сбоев в работе компьютера. Поэтому важно заранее создавать резервные копии ценных данных.

- **Выбор хранилища.** Для резервного копирования можно использовать облачные сервисы, внешние жесткие диски или флеш-накопители. Облачные технологии обеспечивают доступ к файлам с любого устройства, а физические носители позволяют хранить копии в автономном режиме.
- **Создание копий по расписанию.** Чтобы минимизировать потери в случае атаки, следует настраивать автоматическое сохранение важных файлов с определенной периодичностью, например, раз в неделю или при внесении значительных изменений.
- **Хранение копий в защищенном месте.** Важно, чтобы резервные сведения не находились в той же системе, что и оригиналы. Это предотвратит их шифрование при заражении вирусами-вымогателями или случайное удаление.
- **Проверка целостности копий.** Иногда файлы в резервном хранилище могут повреждаться из-за аппаратных сбоев или ошибок записи. Периодическая проверка позволяет убедиться, что данные можно будет восстановить в случае необходимости.

Соблюдение всех этих мер позволяет значительно снизить риск заражения устройства и потери важной информации. Комплексный подход к сбережению данных помогает пользователям чувствовать себя увереннее в цифровом пространстве и минимизировать потенциальные угрозы.

Правила кибергигиены в цифровой среде

Иллюстративное фото / newUROKI.net

> ***Кибергигиена — это** совокупность правил и действий, которые помогают безопасно пользоваться компьютерами, смартфонами, интернетом и цифровыми сервисами. Она включает в себя защиту паролей, осторожность при скачивании файлов, проверку ссылок перед переходом и использование антивирусных программ.*

Определение

Незнание или игнорирование этих правил может привести к утечке конфиденциальной информации, взлому аккаунтов, заражению гаджетов вирусами или даже финансовым потерям.

Безопасное использование паролей

Пароли защищают наши аккаунты и личные данные от несанкционированного доступа. Однако если они слишком простые или используются неправильно, их легко взломать.

Основные правила надежных паролей:

- Минимальная длина — не менее 12 символов. Чем длиннее — тем сложнее его подобрать.
- Использование разных символов — рекомендуется сочетать буквы (заглавные и строчные), цифры и специальные знаки (#, @, %, &). Например, код доступа: P@ssw0rd2024! безопаснее, чем password123.
- Уникальные коды для каждого аккаунта — если злоумышленники взломают один профиль, они не получат доступ к остальным. Использование одного кода для всего — большая ошибка.
- Регулярная смена — рекомендуется обновлять коды доступа хотя бы раз в 3–6 месяцев, особенно для важных аккаунтов (банкинг, соцсети, электронная почта).

Чего нельзя делать:

- Использовать имя, дату рождения или простые комбинации (qwerty, 12345678 и т. д.).
- Хранить пароли в текстовых документах на компьютере или записывать их на листочках.
- Сообщать свои коды доступа друзьям, даже если доверяешь им.

Пример:
Андрей использовал пароль Andrey2008 для всех своих аккаунтов. Однажды его страница в соцсетях была взломана, и мошенники, узнав этот код, получили доступ к его почте и другим сервисам. Чтобы избежать подобных ситуаций, лучше использовать разные коды и хранить их в специальном менеджере.

Правила безопасного скачивания файлов

Часто пользователи скачивают файлы из интернета, не задумываясь об их безопасности. Однако вредоносные объекты часто маскируются под безобидные программы, музыку или документы.

Как скачивать безопасно:

- Использовать только проверенные источники. Если требуется загрузить приложение, лучше делать это через официальные магазины (Google Play, RuStore) или сайты разработчиков.
- Проверять формат файлов. Вирусы часто прячутся в файлах с расширениями .exe, .bat, .scr или .vbs. Если тебе предлагают скачать документ, но его формат подозрительный (например, report.pdf.exe), это, скорее всего, вредоносный объект.
- Читать отзывы. Перед скачиванием лучше посмотреть комментарии других пользователей. Если они жалуются на странное поведение приложения, его лучше не устанавливать.
- Использовать антивирус. Некоторые защитные системы проверяют файлы перед загрузкой и могут предупредить о возможной угрозе.

Чего нельзя делать:

- Скачивать файлы с подозрительных сайтов или по незнакомым ссылкам.
- Открывать вложения в письмах от неизвестных отправителей (об этом подробнее в следующем пункте).
- Игнорировать предупреждения браузера или антивируса о возможной опасности.

Пример:
Марина хотела скачать бесплатную версию популярной игры и нашла сайт с предложением загрузить game_free.exe. После установки её компьютер начал работать медленнее, а на экране стали появляться странные рекламные окна. Оказалось, что она скачала вирус, замаскированный под игру. Чтобы избежать таких ситуаций, лучше скачивать приложения только с официальных источников.

Осторожность при работе с электронной почтой и сообщениями

Мошенники часто используют электронную почту и мессенджеры, чтобы обманом получить личные данные пользователей. Такие атаки называются фишингом.

Как не попасться на уловки:

- Не открывать письма от незнакомцев. Если ты получил странное сообщение с обещанием выигрыша или просьбой срочно что-то сделать, лучше его проигнорировать.
- Проверять адрес отправителя. Иногда злоумышленники подделывают адреса, чтобы письмо выглядело официальным. Например, вместо support@yandex.ru они могут написать support@yandeks.ru . Разница почти незаметна, но это поддельный адрес.
- Не переходить по подозрительным ссылкам. В письме или сообщении может быть ссылка на сайт, который выглядит как настоящий (например, копия страницы банка). Если ты введешь туда свои данные, они попадут к мошенникам.
- Не скачивать вложения без проверки. Даже если файл называется Квитанция.pdf, он может содержать вирус. Если письмо пришло от незнакомого человека, лучше не открывать вложения.

Чего нельзя делать:

- Сообщать персональные идентификаторы, данные банковских карт или личную информацию в ответ на письма или сообщения.
- Вести переписку с подозрительными аккаунтами, которые представляются сотрудниками банков или техподдержки.
- Верить сообщениям о «неожиданном выигрыше» или «срочной блокировке аккаунта» — это обман.

Пример:
Павел получил письмо с уведомлением, что его страница ВКонтакте якобы заблокирована, и для восстановления доступа нужно перейти по ссылке. Он открыл сайт, похожий на оригинальный, и ввел свой логин и пароль. Через несколько минут его аккаунт был взломан, и от его имени начали рассылать спам. Если бы он проверил ссылку перед вводом данных, он бы заметил, что адрес отличается от настоящего vk.com.

Соблюдение правил кибергигиены помогает защитить личные данные, избежать вирусов и мошенничества. Надежные пароли, внимательность при скачивании файлов и осторожность при работе с электронной почтой — это основные шаги к безопасному использованию цифровых технологий.

Таблица: Методы обеспечения цифровой безопасности

Метод	Описание
Использование сложных паролей	Защищает от несанкционированного входа
Регулярное обновление системы	Повышает устойчивость к угрозам
Проверка ссылок перед переходом	Предотвращает переход на мошеннические ресурсы

Ограничение доступа к личной информации	Минимизирует риски утечки сведений
Внимательное отношение к письмам и сообщениям	Помогает избежать обмана

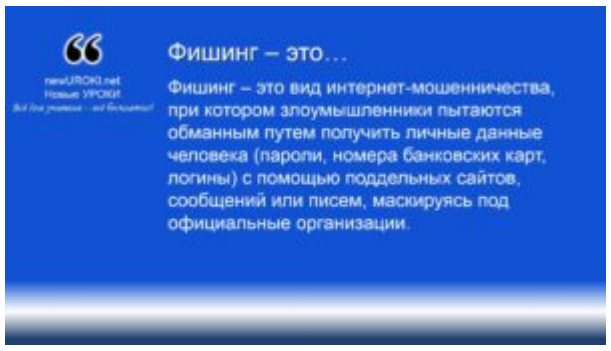
Опасные явления в социальных сетях и мессенджерах

Иллюстративное фото / newUROKI.net

Современные социальные сети и мессенджеры позволяют общаться с друзьями, узнавать новости и обмениваться информацией. Однако вместе с удобством они несут и серьезные риски: мошенничество, кража данных, манипуляции и даже финансовые потери. Чтобы избежать неприятных ситуаций, важно знать основные угрозы и способы защиты.

Фишинговые атаки и социальная инженерия

> ***Фишинг – это** вид интернет-мошенничества, при котором злоумышленники пытаются обманным путем получить личные данные человека (пароли, номера банковских карт, логины) с помощью поддельных сайтов, сообщений или писем, маскируясь под официальные организации.*



Определение

Как это работает:

Человек получает сообщение от «администрации соцсети» с предупреждением, что его аккаунт заблокируют. В письме есть ссылка, ведущая на сайт, внешне похожий на настоящий. Если пользователь введет логин и пароль, эти сведения попадут к злоумышленникам.
Мошенники могут представляться другом или родственником и просить срочно перевести деньги, сославшись на трудности. Например, «Привет, это я, мой телефон утонул, срочно скинь 500 рублей на новую симку».

Как не попасться на фишинг:

- Не переходить по подозрительным ссылкам, даже если сообщение выглядит официально.
- Проверять адрес отправителя. Если он странный или похож на оригинальный (например, support@wk.com вместо support@vk.com), это обман.
- Задавать уточняющие вопросы. Если пишет друг и просит денег, лучше позвонить ему и проверить информацию.

Пример:
Олег получил письмо якобы от VK с предупреждением о блокировке аккаунта. В письме была ссылка для подтверждения данных. Олег перешел по ней, ввел логин и пароль, после чего потерял доступ к своему профилю. Это был фишинг, и злоумышленники украли его страницу.

Мошенничество в социальных сетях

Обман в соцсетях бывает разным: от поддельных розыгрышей до кражи денег через фальшивые интернет-магазины.

Виды мошенничества:

- **Фальшивые розыгрыши и подарки.** Вам пишут, что вы выиграли телефон, но для получения приза нужно оплатить «налог» или «доставку». После перевода денег мошенники исчезают.
- **Поддельные интернет-магазины.** Они предлагают дорогие вещи по заниженным ценам, но после оплаты товар не приходит.
  Взломанные аккаунты друзей. Вам пишет знакомый с просьбой занять денег. На самом деле это мошенник, получивший доступ к его странице.

Стоит прочесть также: Безопасность бытовых приборов - конспект урока

Как защититься:

- Не переводить деньги незнакомцам, даже если предложение кажется выгодным.
- Проверять сайты перед покупкой (читать отзывы, искать контактные реквизиты).
- Настроить двухфакторную аутентификацию, чтобы защитить свой аккаунт от взлома.

Пример:
Лена увидела в соцсети рекламу нового Huawei за 5 000 рублей. Она перевела деньги, но смартфон так и не получила. Оказалось, что это был фальшивый магазин.

Защита персональных данных в социальных сетях

Чем больше информации человек публикует о себе в интернете, тем легче мошенникам использовать её против него.

Как защитить свои данные:

- Ограничить видимость профиля — закрыть аккаунт или настроить приватность так, чтобы посторонние не видели личную информацию.
- Не выкладывать слишком много сведений — дату рождения, адрес, номер телефона лучше скрыть.
- Не делиться геолокацией в реальном времени — если вы на отдыхе, лучше выложить фото после возвращения, а не во время поездки.

Чего нельзя делать:

- Выкладывать фото банковских карт, билетов, паспортов.
- Оставлять пароли в открытом доступе или передавать их другим людям.
- Добавлять в друзья незнакомцев и делиться с ними личной информацией.

Пример:

Ваня часто выкладывал фото с геолокацией, отмечая, когда он дома и когда уезжает в путешествие. Однажды, когда он был в отпуске, его квартира была ограблена. Мошенники узнали, что никого нет дома, просто следя за его соцсетями.

Социальные сети и мессенджеры могут быть опасны, если не соблюдать меры предосторожности. Фишинг, мошенничество и утечка данных — самые распространенные угрозы, с которыми сталкиваются пользователи. Чтобы избежать проблем, важно соблюдать правила безопасности и быть внимательными к подозрительным сообщениям, незнакомым сайтам и излишнему распространению личной информации.

Практические навыки защиты в цифровой среде

Иллюстративное фото / newUROKI.net

Один из ключевых навыков безопасного поведения в интернете — умение распознавать потенциально опасные файлы и ссылки. Вредоносные объекты часто маскируются под безобидные изображения, документы или программы, но их запуск может привести к заражению устройства.

Чтобы не стать жертвой кибератак, нужно соблюдать несколько простых правил:

- Не открывать файлы и гиперссылки от незнакомых отправителей. Например, если вам в соцсети написал человек, которого вы не знаете, и прислал видео с подписью «Срочно посмотри!», не спешите скачивать его. Сначала уточните, кто это, и почему он отправил его.
- Проверять ссылки перед переходом. Если вам пришло сообщение с подозрительной ссылкой, наведите на нее курсор (не нажимая) и посмотрите, куда она ведет. Например, вместо официального сайта банка sberbank.ru мошенники могут подменить адрес на sberbank-login.ru — такой сайт будет фальшивым.
- Использовать онлайн-сервисы для проверки гиперссылок и файлов. Например, сайт **Лаборатория Касперского*** позволяет загружать файлы или вставлять ссылки, чтобы проверить их на наличие угроз.
- Настроить отображение расширений документов в системе. Если он называется «Презентация.pptx.exe», то это не настоящий файл PowerPoint, а программа, которая может навредить вашему устройству.

> ***АО «Лаборатория Касперского»** — международная компания, специализирующаяся на разработке систем защиты от компьютерных вирусов, спама, хакерских атак и прочих киберугроз. Компания ведёт свою деятельность более чем в 200 странах и территориях мира. Центральный офис «Лаборатории Касперского» находится в Москве. Сайт*

Настройка двухфакторной аутентификации

Одним из самых эффективных способов защиты аккаунтов является двухфакторная аутентификация (2FA). Она добавляет дополнительный уровень безопасности при входе в учетные записи, требуя не только пароль, но и подтверждение с помощью кода из SMS, специального приложения или аппаратного ключа.

Как включить 2FA:

- Войти в настройки аккаунта (например, в соцсети или электронной почте).
- Найти раздел «Безопасность» или «Двухэтапная аутентификация».
- Выбрать способ подтверждения:

1. Код по SMS (менее безопасно, но лучше, чем ничего).
2. Код через специальное приложение (например, Google Authenticator или Authy).
3. Аппаратный ключ (используется в корпоративных системах).

- Подключить и сохранить резервные коды, которые помогут восстановить доступ в случае утери телефона.

Пример:

Допустим, кто-то узнал ваш пароль от Вконтакте и пытается войти в ваш аккаунт с чужого устройства. Если у вас включена 2FA, система запросит дополнительный код, который придет только вам, и злоумышленник не сможет получить доступ.

Действия при обнаружении признаков заражения устройства

Если ваш компьютер или смартфон начал вести себя странно — тормозит, открывает лишние окна, самопроизвольно отправляет сообщения друзьям — возможно, он заражен вредоносным кодом.

В такой ситуации важно действовать быстро:

- Отключить интернет. Это поможет предотвратить утечку данных и дальнейшее распространение вредоносных элементов.
- Запустить полную проверку антивирусом. Используйте проверенное защитное ПО, чтобы обнаружить и удалить угрозу.
- Удалить подозрительные программы и файлы. Если на устройстве появились неизвестные приложения, которые вы не устанавливали, их нужно немедленно удалить.
- Сменить пароли. Если вы вводили учетные данные на подозрительных сайтах, нужно обновить пароли ко всем важным сервисам.
- Обратиться к специалисту. Если ситуация кажется сложной и самостоятельно справиться не удается, лучше показать устройство IT-специалисту.

Пример:

Представьте, что друг пишет вам в мессенджере: «Ты тут на видео смешно выглядишь, посмотри!» и присылает ссылку. Вы переходите по ней, а сайт просит ввести логин и пароль от соцсети. Если вы это сделаете, ваш аккаунт попадет в руки злоумышленников, которые начнут рассылать такие же сообщения вашим друзьям. Чтобы этого не произошло, важно соблюдать все перечисленные меры предосторожности.

Соблюдение правил цифровой безопасности помогает избежать множества угроз. Проверяя подозрительные ссылки, используя двухфакторную аутентификацию и зная, как реагировать на подозрительные признаки на устройстве, каждый человек может защитить свои данные и сохранить личную информацию в безопасности.

Рефлексия

Дорогие девятиклассники, давайте проведём рефлексию. Сегодня мы узнали, как проверять подозрительные файлы и ссылки, зачем нужна двухфакторная аутентификация и какие действия необходимо предпринять, если устройство заражено вредоносным кодом.

Сейчас мне важно узнать, как вы оцениваете свою работу и усвоенный материал. Для этого ответьте на несколько вопросов:

- Какую информацию этого занятия вы считаете самой полезной для себя?
- Что из изученного вы точно будете применять в повседневной жизни?
- Какие моменты показались вам сложными или непонятными?

(Учитель дает ученикам время на размышление, после чего предлагает несколько способов выразить свои мысли.)

Метод «Светофор»

- Если вам все было понятно, и вы уверены, что сможете применять знания на практике — поднимите зеленую карточку.
- Если материал понятен, но у вас остались небольшие вопросы — желтую карточку.
- Если было сложно, и нужно повторение — красную карточку.

Метод «Закончите фразу»

Я попрошу вас закончить одно из предложений:

- «Сегодня на уроке я понял(а), что…»
- «Больше всего меня удивило то, что…»
- «Теперь я знаю, как…»

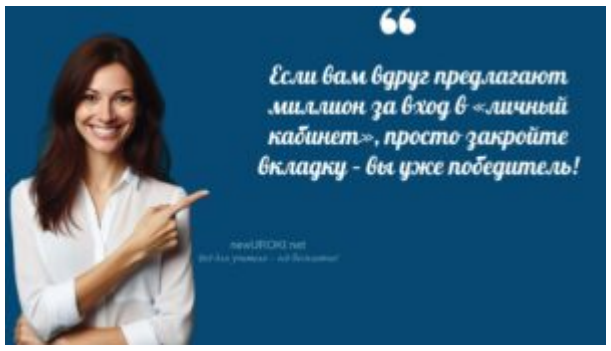
Метод «Лесенка»

Нарисуйте в тетради лестницу из трех ступенек и напишите на них:

- Что я уже знал(а) по теме занятия?
- Что нового узнал(а)?
- Как я могу использовать эти знания в жизни?

(Учитель слушает ответы учеников, подводит итог, еще раз акцентирует внимание на ключевых моментах.)

Заключение



Учителя шутят

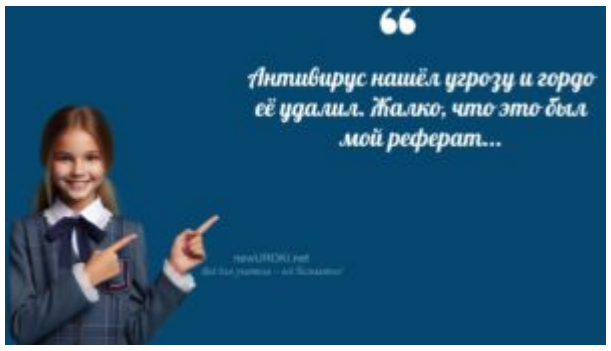
Сегодня мы с вами поговорили о том, как защитить свою цифровую среду и избежать нежелательных ситуаций при работе с технологиями. Современный мир предлагает нам невероятные возможности для общения, учебы и творчества, но вместе с этим он требует от нас ответственности и осознанности.

Представьте, что ваш гаджет — это ваш личный помощник. Насколько он будет надежным, зависит от того, как вы о нем заботитесь. Если соблюдать простые, но важные правила безопасности, вы сможете избежать множества неприятностей.

Каждый из вас — не просто пользователь интернета, а его активный участник. Именно от ваших действий зависит, насколько комфортным и защищенным будет ваше пространство в сети. Будьте внимательны, критически оценивайте информацию, не доверяйте незнакомцам и не спешите нажимать на сомнительные ссылки.

Знания, которые вы получили сегодня, — это не просто теория. Это реальные навыки, которые помогут вам чувствовать себя уверенно в цифровой среде. Используйте их, делитесь с близкими, и помните: безопасность — это не ограничение, а свобода!

Домашнее задание



Ученики шутят

Обязательная часть:

- Составить памятку «Мои правила безопасности в интернете» (не менее 5 пунктов)
- Выполнить установку антивирусной программы на домашнем компьютере (с разрешения родителей)

По желанию:

- Подготовить презентацию об одном из видов вредоносных приложений
- Создать инфографику «Признаки заражения устройства вредоносной программой»

Технологическая карта

Скачать бесплатно технологическую карту урока по теме: «Вредоносные программы и приложения, способы защиты от них. Опасные программы и явления цифровой среды»

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: «Вредоносные программы» в формате Ворд

Чек-лист педагога

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

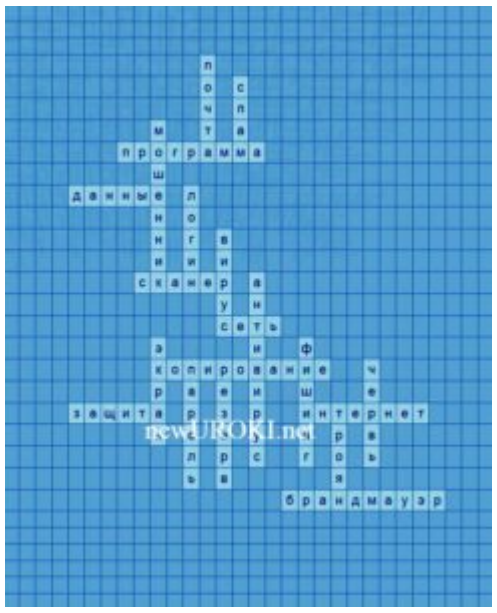
Чек-лист для преподавателя — это инструмент педагогической поддержки, представляющий собой структурированный перечень задач, шагов и критериев, необходимых для успешного планирования, подготовки и проведения урока или мероприятия.

Карта памяти для учеников

Скачать бесплатно карту памяти для учеников 9 класса по ОБЗР по теме: «Вредоносные программы» 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: «Вредоносные программы и приложения, способы защиты от них. Опасные программы и явления цифровой среды» в формате WORD

Тесты

Что такое фишинг?

а) Вид рыбной ловли

б) Метод кражи личной информации через подложные сайты

в) Название компьютерной игры

Правильный ответ: б

Что рекомендуется делать для безопасности в интернете?

а) Использовать один и тот же пароль везде

б) Открывать письма от незнакомых отправителей

в) Регулярно обновлять антивирусное ПО

Правильный ответ: в

Как распознать зараженное устройство?

а) Нормальная работа без изменений

б) Появление незнакомых всплывающих окон

в) Увеличение скорости работы устройства

Правильный ответ: б

Что такое двухфакторная аутентификация?

а) Вид компьютерной игры

б) Дополнительный способ подтверждения личности

в) Настройка электронной почты

Правильный ответ: б

Как безопасно скачивать контент?

а) Качать из любых источников

б) Проверять источник и репутацию сайта

в) Скачивать без проверки

Правильный ответ: б

Что делать при подозрении на заражение?

а) Продолжать использовать устройство

б) Отключить от интернета и проверить антивирусом

в) Удалить все фотографии

Правильный ответ: б

Какой пароль считается надежным?

а) 12345

б) Имя домашнего питомца

в) Сложная комбинация символов

Правильный ответ: в

Риск социальной инженерии это:

а) Изучение социологии

б) Манипуляция людьми для получения информации

в) Общение в социальных сетях

Правильный ответ: б

Что такое брандмауэр?

а) Система безопасности компьютера

б) Название огнетушителя

в) Вид компьютерной игры

Правильный ответ: а

Как часто нужно создавать резервные копии?

а) Раз в год

б) Никогда

в) Регулярно, желательно еженедельно

Правильный ответ: в

Интересные факты для занятия

1. **Интересный факт 1:**
   В 2017 году хакерская атака вируса WannaCry парализовала работу более 200 000 компьютеров в 150 странах мира, включая крупнейшие больницы, железные дороги и даже правительственные учреждения. Общий ущерб составил около 4 миллиардов долларов!
2. **Интересный факт 2:**
   Средний подросток ежедневно проводит в интернете около 7 часов, при этом только 32% из них знают базовые правила кибербезопасности. Каждый второй подвергается риску кражи личной информации.
3. **Интересный факт 3:**
   Самый дорогой киберпреступник в мире — Пётр Левашов (известный как «Peter Severa»), который заработал на киберпреступлениях более 100 миллионов долларов. Он был задержан испанскими спецслужбами в 2017 году и осужден к лишению свободы.

Интеллект-карта

Ментальная карта (интеллект-карта, mind map)

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

Облако слов

Облако слов

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

Презентация

Презентация

Скачать бесплатно презентацию на урок ОБЗР в 9 классе по теме: «Вредоносные программы и приложения, способы защиты от них. Опасные программы и явления цифровой среды» в формате PowerPoint

БОНУС: Рабочий лист

Скачать бесплатно рабочий лист по ОБЗР по теме: «Вредоносные программы и приложения, способы защиты от них. Опасные программы и явления цифровой среды» 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. Щукин В.Н., Фельковский А.К. «Основы цифровой грамотности». Издательство «Сириус», Санкт-Петербург, 2005. 224 страницы.
2. Сергейчук И.П. «Безопасность информационной среды: основы и риски». Издательство «Научная перспектива», Москва, 2004. 198 страниц.
3. Якушев О.Л., Михайлова Т.В. «Современные технологии в сфере коммуникации». Издательство «Альфа-Книга», Казань, 2002. 175 страниц.
4. Луковская Р.М., Орлова Е.Н. «Цифровая эра: перспективы и угрозы». Издательство «Техно-Пресс», Новосибирск, 2001. 210 страниц.
5. Тополев С.Ю. «Интернет и его влияние на общество». Издательство «Инфо-Глобус», Екатеринбург, 2003. 190 страниц.

Слова ассоциации (тезаурус) к уроку: информация, система, код, сигнал, угроза, сеть, вирус, пароль, доступ, контроль, технология, риск, блокировка.

Цифровая среда — 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.

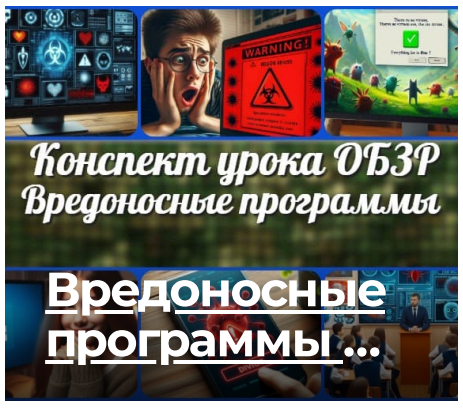
ПОХОЖИЕ УРОКИ

Цифровая среда — ...

Защита прав в цифровом...

Достоверность информац...

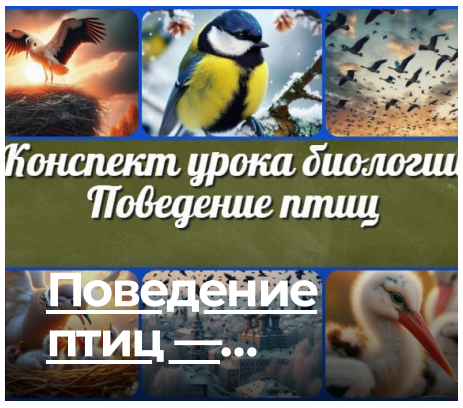
ИНТЕРЕСНЫЕ КОНСПЕКТЫ УРОКОВ



Вредоносные программы ...

Цифровая среда — ...

Общая характеристи...



Поведение птиц — ...

Новые УРОКИ

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