

Всероссийский конкурс творческих, учебно-образовательных,
исследовательских, научно-популярных проектов
«Научно-образовательного центра педагогических проектов»

Методическая разработка урока по учебному предмету «Информатика» в
рамках программы основного общего и среднего общего образования

Вид работы: план-конспект урока

Название работы: «Сервисы интернет-коммуникаций. Сетевой этикет.
Стратегии безопасного поведения в Интернете»

Автор: Шараева Наталья Викторовна

Место работы автора: ОГАОУ «Интеграция»

Должность: учитель информатики

Томск-2026

Описание технологической идеи

урока информатики в 7-м классе по теме «Сервисы интернет-коммуникаций. Сетевой этикет. Стратегии безопасного поведения в интернете».

Тема урока: «Сервисы интернет-коммуникаций. Сетевой этикет. Стратегии безопасного поведения в интернете»

Возраст обучающихся: 13-14 лет

Класс: 7 класс

Цель урока: формирование знаний обучающихся о современных сервисах интернет-коммуникаций, правилах сетевого этикета и способах обеспечения безопасности в сети Интернет.

Задачи урока:

1. Ознакомить с разнообразием интернет-сервисов и особенностями их использования.
2. Развивать навыки анализа и оценки риска, связанный с общением в сети.
3. Сформировать четкое представление о принципах сетевого этикета и уважительного общения.
4. Способствовать развитию осознанного подхода к защите персональных данных и предупреждению негативных последствий онлайн-деятельности.

Планируемые результаты:

- Предметные: обучающиеся научатся различать основные виды сервисов интернет-коммуникаций, понимать правила сетевого этикета и стратегии безопасного поведения в интернете.

- Метапредметные: развитие коммуникативных навыков, критического мышления, умения анализировать и оценивать риски, связанные с использованием интернета.

- Личностные: формирование осознанной позиции по вопросам личной безопасности и этичного поведения в цифровом мире.

Место в тематическом разделе: тема урока является заключительной в тематическом 1 разделе «Цифровая грамотность»

Ведущие понятия: аккаунт, логин, пароль, электронная почта, мессенджер, видеоконференц-связь, социальная сеть, сетевой этикет, личная информация, безопасность в Интернете.

Тип урока:

Открытия нового знания и первичного закрепления.

Методы обучения:

- Словесные методы (беседа, рассказ, обсуждение).

- Наглядные методы (демонстрация примеров сетевых коммуникаций, видеороликов о безопасности в интернете).

- Практические методы (выполнение практических заданий по работе с сервисами интернет-коммуникаций, работа с кейсами по соблюдению сетевого этикета и стратегий безопасного поведения).

Средства обучения:

- Компьютеры/планшеты с доступом в интернет.

- Презентация учителя по теме занятия (Приложение 1).

- Примеры реальных ситуаций взаимодействия через сервисы интернет-коммуникаций.

- Кейсы и задания для групповой работы.

Средства контроля на уроке:

- Фронтальный опрос.
- Индивидуальный опрос.
- Проектная деятельность.
- Рефлексия.

Формы работы обучающихся: индивидуальная и групповая.

Формы организации познавательной деятельности обучающихся: фронтальная, самостоятельная, парная.

Принципы обучения: систематичности и последовательности, наглядности, доступности, связи теории с практикой.

Информационно-образовательная среда: интерактивная панель, компьютерная презентация, ПК обучающихся, оценочные листы.

Средства обучения: раздаточный материал, содержащий задания по формированию функциональной грамотности.

Педагогические технологии: информационно-коммуникационная технология, технология деятельностного метода.

Ход урока:

1. Организационный этап (3 минуты):

Деятельность учителя.

Приветствие, проверка присутствующих, постановка целей и задач урока.

Обучающие и развивающие компоненты, задания и упражнения:

- создание рабочей атмосферы, настрой на продуктивную деятельность.
- развитие самоорганизации и умения быстро переключаться на учебную деятельность.

Учитель приветствует обучающихся. Проверяет готовность обучающихся к уроку, проверка подготовки домашней работы, тетради, ручки.

Деятельность обучающихся.

В результате: обучающиеся приветствуют учителя, проверяют наличие необходимых учебных материалов (учебник, тетрадь, ручка). Эмоционально настраиваются на урок.

Работа с УУД:

Регулятивные УУД:

Самоорганизация (контроль готовности к уроку).

Коммуникативные УУД:

Готовность к слушанию и взаимодействию.

Личностные УУД:

Положительный настрой на учебную деятельность.

2. Актуализация знаний, подведение к теме урока (5–7 минут):

Деятельность учителя.

Создание проблемной ситуации

Стартовая задача:

Учитель:

слайд 2.

Ребята, у каждого может быть такая ситуация:

Ваш друг просит перейти по неизвестной ссылке для голосования, угрожая последствиями, если не выполните его просьбу.

Вопросы для обсуждения:

- Что бы вы сделали в подобной ситуации?
- Какие последствия возможны при переходе по сомнительным ссылкам?

Задания для учеников:

- Индивидуальное решение проблемы.
- Обмен мнениями в парах.

Цель этапа:

Формирование умения анализировать потенциальные угрозы и предотвращать рискованные действия в сети.

Вопрос учителя: Что сделаете?

1. Пройдете по предложенной ссылке
2. Отправите другу сообщение, чтобы проверить
3. Не обратите на сообщение внимание

слайд 3.

Вопрос учителя: Какими могут быть последствия

Учитель: Теперь прошу предложить высказать свое мнение по вопросу «Какие последствия перехода по незнакомым ссылкам могут быть?»:

При выборе 1 - ваш аккаунт будет взломан, персональные данные похищены

При выборе 2 - вы узнаете, что его аккаунт взломан

При выборе 3 - вы в безопасности, но друг в беде

Вопрос учителя: Какие выводы можем сделать?

Учитель: Чтобы всегда делать правильный выбор, нужно знать:

Какими сервисами можно пользоваться безопасно и как отличить их от поддельных сайтов.

Как проявлять уважение в общении.

Как заметить угрозу.

Тема нашего занятия:

«Сервисы интернет-коммуникаций. Сетевой этикет. Стратегии безопасности»

Наша цель - научиться принимать правильные решения в интернете!

Деятельность обучающихся.

Анализируют проблемную задачу «Опасность в сети».

Обдумывают свой опыт.

Говорят о своих вариантах развития события, отвечают на вопросы учителя, аргументируя свои ответы.

Работа с УУД:

Регулятивные УУД:

- целеполагание (формулировка целей урока).
- планирование (определение шагов для достижения целей).

Познавательные УУД:

- анализ проблемной ситуации.
- синтез (установление причинно-следственных связей в истории поставленной задачи).
- выдвижение гипотез (предположение о теме урока).

Коммуникативные УУД:

- умение выражать свою точку зрения.
 - ведение учебного диалога с учителем и одноклассниками.
- Личностные УУД:
- смыслообразование (осознание личной значимости темы).
 - нравственно-этическое оценивание (оценка поступков героя ситуации).

Обзор основных понятий, связанных с интернетом и коммуникациями, повторение ранее изученного материала.

3. Изучение нового материала (15–20 минут):

3.1. Актуализация личного опыта обучающихся в использовании интернет-сервисов.

Деятельность учителя.

Учитель: Давайте проведем небольшую разминку. Я прошу вас назвать все способы и приложения, которые вы используете для общения в Интернете. Не стесняйтесь, называйте все, что приходит в голову!

(Ученики активно называют: МАХ, Telegram, ВКонтакте, Сферум, Zoom), чаты в онлайн-играх, электронная почта и т.д.).

Учитель: Как видите, спектр сервисов огромен. Все это – сервисы интернет-коммуникаций. Давайте изучим их подробнее.

Деятельность обучающихся.

Участвуют в «мозговом штурме»: активно называют все известные им сервисы и приложения для общения.

Работа с УУД:

Личностные:

- развивают познавательный интерес к техническим дисциплинам, ответственно относятся к учебе, имеют мотивацию к учебной деятельности
- развитие умения структурировать известную информацию, выделять общее и частное.

Познавательные:

- извлекают информацию из прослушанного объяснения учителя, анализируют ее; Коммуникативные: умеют слушать учителя и одноклассников, формулировать вопросы, делать выводы.

3.2. Открытие нового знания. Практическая деятельность.

Деятельность учителя.

Организовать самостоятельное «открытие» нового знания через работу с информацией в группах.

Развитие навыков работы в команде (коммуникация, распределение ролей, договоренность), анализа текста, выделения главного, структурирования и представления информации.

Учитель: Теперь мы поработаем в группах. Каждая группа получит свое задание и материал для изучения. У вас есть 7-8 минут на подготовку и 2-3 минуты на презентацию вашего результата.

(Класс делится на 3 группы. У каждой группы есть ноутбук. На ноутбуке сохранена папка с материалами и заготовками файлов для работы (таблица для заполнения, направляющий текст) для записи результатов и оформления. Учитель раздает каждой группе задание и раздаточный материал). В раздаточном материале карточки с названием роли ученика в группе и перечень заданий. Роли: спикер – представляет результат работы

в группе, секретарь – записывает результаты работы, художник – оформляет в интересном собственном стиле, хронометрист – следит за временем. Каждый участвует в обсуждении.

Деятельность обучающихся.

Организационный этап в группе. распределяют роли.

Изучают предложенный раздаточный материал: внимательно читают, выделяют ключевые идеи.

Работа в малых группах (3 группы): слайд 4

Группа	Задача
Исследователи	Определение видов интернет-коммуникаций (синхронные и асинхронные сервисы)
Цифровые защитники	Составление списка рекомендаций по защите персональных данных
Эксперты этикета	Создание памятки по правилам сетевого этикета

Организация деятельности:

Каждая группа получает инструкции и самостоятельно решает поставленную задачу, используя цифровые инструменты и собственный опыт.

Завершение этапа:

- Выступления представителей каждой группы перед классом.
- Совместное обсуждение полученных выводов.

Работа с УУД:

- Познавательные: обработка информации, выявление закономерностей.
- Коммуникативные: взаимодействие в коллективе, выражение мыслей.
- Регулятивные: самоконтроль, оценка качества выполненных заданий.

4. Первичное закрепление (3-4 минут)

Деятельность учителя.

Систематизировать и корректировать знания, полученные группами, обеспечить усвоение материала всеми учащимися.

Развитие монологической речи, умения слушать, задавать вопросы, корректировать и дополнять ответы одноклассников.

Интерактивные задания:

слайд 5-9

- Тест-кейс «Узнай мошенника!»: определение признаков потенциально опасных сообщений (Приложение 2).

слайд 10-11

- Упражнения по составлению правильного пароля и оценке его надежности (Приложение 3).

Особенности организации:

Практический тренинг позволяет закрепить теоретические знания, развить навыки критического мышления и анализа рисков.

Работа с УУД:

Коммуникативные УУД:

- владение монологической речью (выступление спикера).
- владение диалогической речью (ответы на вопросы, участие в обсуждении).
- умение слушать и слышать выступления других групп.

Познавательные УУД:

- структурирование знаний (конспектирование ключевых идей в тетрадь).
- смысловое чтение (восприятие и анализ информации со слайдов).
- установление причинно-следственных связей (между ошибками Саши и изучаемыми правилами).

Регулятивные УУД:

- контроль (сравнение результатов своей группы с другими и с эталоном учителя).

5. Рефлексия (3 минуты):

Оценивание учениками собственных достижений, определение уровня усвоенных знаний и компетенций.

Деятельность учителя.

Ребята, на ваших столах лежат листы обратной связи. Предлагаю необычное завершение нашего урока:

Слайд 12

Рефлексия «Автопортрет киберсупергероя»

Задача:

Представьте себе, что вы стали супергероем интернета, обладающим особыми навыками безопасного поведения и сетевого этикета. Нарисуйте автопортрет своего персонажа и дополните рисунок следующими деталями:

1. «Имя кибергероя»: Придумайте название своему персонажу, отражающее вашу осведомленность в области цифровых технологий и желание помогать другим пользователям сети.

Например: «Защитник Данных», «Этикет-Мэн», «Паролец-Профи».

2. «Специальные способности»: Опишите уникальные навыки, которыми обладает ваш персонаж для борьбы с угрозами в интернете (например, защита от вирусов, быстрое обнаружение фальшивых аккаунтов, обучение пользователей правильному поведению в сети).

3. «Идеальные гаджеты»: Напишите или нарисуйте устройства или предметы, помогающие герою эффективно защищать интернет-пространство (например, шлем шифрования, рюкзак антивирусных патчей, перчатки быстрого реагирования).

4. «Совет друзьям»: Запишите краткий слоган или призыв, которым герой вдохновляет других пользователей соблюдать сетевой этикет и заботиться о безопасности.

6. Домашнее задание (1 минута):

Слайд 13

Создать инфографику на тему безопасности в сети с элементами дизайна, отображающими ваши рекомендации и советы.

7. Подведение итогов урока (2–3 минуты):

Деятельность учителя.

Определить уровень овладения материалом и настроение учеников.

Учитель развивает у учащихся умения самооценки и рефлексивного анализа, а также формирует способность объективно оценивать собственные успехи. По завершении урока преподаватель суммирует пройденное, благодарит участников за активную работу, объявляет отметки и даёт пояснения к домашнему заданию.

Деятельность обучающихся.

Анализируют свою работу на уроке, оценивают работу в группах

Осознание степени усвоения материала, анализ собственных трудностей и успехов, формирование личного отношения к изученному материалу

Работа с УУД:

Личностные: обладают умениями оценки своей деятельности

Регулятивные: оценивают свою работу на уроке, умеют адекватно воспринимать информацию учителя или товарища, содержащую оценочный характер отзыва о работе на уроке.

Коммуникативные: умеют излагать свое мнение и аргументировать свою точку зрения

Список используемой литературы и источников:

1. Босова Л.Л., Информатика, 7-й класс: базовый уровень: учебник/ Л.Л. Босова, А.Ю. Босова. 5-е изд., перераб. – Москва: Просвещение, 2023. – 254 с.
2. Босова Л.Л., Информатика. 7-9 классы. Компьютерный практикум. Базовый уровень, Москва: Просвещение, 2025. – 192 с.
3. Федеральная рабочая программа основного общего образования «Информатика (базовый уровень)» https://edsoo.ru/wp-content/uploads/2025/07/2025_ooo_frp_informatika-7-9_baza.pdf.
4. Методические рекомендации по формированию функциональной грамотности обучающихся 5-9 классов с использованием открытого банка заданий на цифровой платформе по шести направлениям функциональной грамотности в учебном процессе и для проведения внутришкольного мониторинга формирования функциональной грамотности обучающихся https://edsoo.ru/wp-content/uploads/2023/08/metodicheskie-rekomendaczii_fg_2022_itog.pdf.

Приложение 1

Сервисы интернет-коммуникаций. Сетевая этикет. Стратегия безопасности

Ирина Н.Н., учитель информатики
© 2020, ООО «ИТЭКО»

Ситуация:

Ваш друг просит поработать по электронной ссылке для рисования, укажите последствия, если вы нажмете на эту ссылку.

Что может?

1. Проверит на предметный сайт;
2. Откажет другу сообщением, чтобы поработать;
3. Не обратит на сообщение внимания

Ситуация №1:

Понимает ли ситуация человек, который готовит и передает данные в интернет-приложение? Почему человек должен знать, какие из них и другим сообщать, чтобы не навредить себе?

А. Безопасные сообщения. Стоит сразу поделиться информацией с друзьями.

Б. Небезопасные сообщения. Безопасно, но лучше бы делиться с друзьями доступом к своим данным.

Мотивация:

Задача №1. Оценка важности своего пароля

«Свой собственный пароль, использовать в различных целях. Свои же данные и на различных ресурсах»

Пароль – это ключ к вашей информации. Если вы не знаете, как его использовать, вы можете потерять доступ к своим данным.

Ситуация №2:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Ситуация №3:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Антипортрет киберсуверенитет

Задача:

Представьте себе, что вы стали свидетелем инцидента, связанного с киберсуверенитетом. Ваши действия должны быть направлены на то, чтобы защитить свои данные и информацию.

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Мотивация:

Задача №1. Оценка важности своего пароля

«Свой собственный пароль, использовать в различных целях. Свои же данные и на различных ресурсах»

Пароль – это ключ к вашей информации. Если вы не знаете, как его использовать, вы можете потерять доступ к своим данным.

Ситуация №4:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Ситуация №5:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Ситуация №6:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Ситуация №7:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Ситуация №8:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Ситуация №9:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Ситуация №10:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Ситуация №11:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Ситуация №12:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Ситуация №13:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Ситуация №14:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Ситуация №15:

Вы хотите посмотреть на Google! Просто кликнув мышью и введя свой логин и пароль, чтобы посмотреть видео?

А. Безопасные сообщения. Просто ввести пароль.

Б. Опасные сообщения. Нужно сначала проверить, что это за сайт, и только потом вводить пароль.

Тест-кейс «Узнай мошенника!»

Этот тест поможет тебе научиться распознавать признаки подозрительных сообщений и защитить себя от возможных угроз в интернете.

Инструкция:

Прочитай каждое сообщение внимательно и выбери один правильный вариант ответа о том, является ли оно опасным или безопасным. Обрати внимание на такие детали как ссылки, грамматические ошибки, просьбы о деньгах или личных данных, а также чувство срочности или страха, которое может вызвать сообщение.

Сообщение №1:

Привет! Я случайно нашёл твой аккаунт и заметил ошибку в настройках приватности. Нужно срочно поменять пароль, иначе кто-то другой сможет получить доступ к твоим данным!

- **А.** Безопасное сообщение. Стоит сразу последовать рекомендациям отправителя.
- **Б.** Подозрительное сообщение. Возможно, это попытка фишинга — получения доступа к моим личным данным.

Правильный ответ: Б.

Сообщение №2:

Ты выиграл поездку на Гавайи! Просто кликни сюда и введи свои личные данные, чтобы подтвердить участие.

- **А.** Безопасное сообщение. Вдруг правда повезло?
- **Б.** Опасное сообщение. Обычно подобные предложения являются обманом и могут привести к потере денег или информации.

Правильный ответ: Б.

Сообщение №3:

Я друг твоей сестры и мне нужна помощь прямо сейчас. У меня проблемы с деньгами, поэтому пришли мне немного через банковский перевод.

- **А.** Безопасное сообщение. Почему бы не помочь другу?
- **Б.** Потенциально опасное сообщение. Лучше сначала связаться со своей сестрой напрямую и уточнить ситуацию.

Правильный ответ: Б.

Выводы:

Мошенники часто используют методы социальной инженерии, создавая ощущение срочности или угрозы, чтобы заставить тебя действовать быстро, не задумываясь. Всегда будь внимателен и осторожен при получении подобных сообщений. Помни сетевые правила безопасного поведения: никому не передавай свою личную информацию и деньги без проверки достоверности источника сообщения.

Составление надежного пароля

Пароли нужны нам каждый день – чтобы зайти в социальные сети, почту, игры, различные сайты и сервисы. Но далеко не каждый пароль достаточно надежен! В этом задании мы научимся составлять безопасные пароли и оценивать их надежность.

Задание №1. Основные правила создания надежных паролей

Прочитай внимательно правила и заполни пропуски в предложениях ниже.

- Пароль должен быть **не менее** _____ символов длиной.
- Чем больше разных типов символов используется (буквы разного регистра, цифры, специальные символы), тем пароль _____.
- Нельзя использовать свои личные данные (имя, фамилию, дату рождения, номер телефона) в качестве пароля.
- Пароль следует менять каждые _____ месяцев.
- Один и тот же пароль нельзя использовать сразу на нескольких сайтах или сервисах.

Заполни пропуски цифрами или словами так, чтобы предложения стали верными утверждениями о создании безопасного пароля.

Задание №2. Оценка надежности своего пароля

1. Создай собственный пароль, используя рекомендации выше.
2. Оцени его надежность по следующим критериям:

Критерий оценки	Баллы
Длина пароля	
Разнообразие символов (прописные буквы, строчные буквы, цифры, спецсимволы)	
Отсутствие личных данных	
Легкость запоминания	

Максимально возможная оценка – 4 балла за каждый критерий, итого максимально можно набрать 16 баллов.

После заполнения таблицы посчитай общую сумму своих баллов и запиши ее: _____ бал(л/ла)

Оценивай себя честно!