

Технологическая карта онлайн-урока
Информатики и ИКТ
7 класс

*Учителя: Милованова Галина Александровна,
Окунева Надежда Евгеньевна*

Предмет: Технология (информатика и ИКТ)

Тема: «Информационная безопасность в сети»

Тип урока: Комбинированный урок

Цель урока: Профилактика правонарушений при работе в сети Интернет, повышение безопасности и правовой защищенности в сети интернет

Планируемые результаты:

Предметные: выделение информационных процессов в социальных системах; проблем, возникающих при развитии информационной цивилизации, и возможные пути их разрешения.

Метапредметные: повышение уровня осведомленности учащихся о наиболее актуальных интернет-угрозах; формирование навыков повседневного использования Интернета и электронных устройств, применяя правила безопасности.

Личностные: формирование навыков соотношения получаемой информации с принятыми в обществе правилами поведения в Интернете; умение обеспечивать защиту значимой информации и личную информационную безопасность.

Условия обеспечения учебной деятельности: персональные компьютеры (для учителя, для учащихся), презентация «Информационная безопасность в сети» <https://disk.yandex.ru/i/Vmu3wJXN0YtHag> , тест (приложение 1), памятки для учащихся (приложение 2).

Этапы урока	Деятельность учителя	Деятельность учащихся	Формируемые УУД	Формы и методы здоровьесберегающей деятельности
<i>Организационный момент</i> (1 мин)	Приветствие учащихся, проверка готовность к занятию, организация внимания	Приветствуют учителя, организуют свое рабочее место		Соблюдение СанПиН и правил охраны труда (Экраны монитора с экраном Retina, как профилактика усталости глаз, правильное сидячие положение перед компьютером.
<i>Актуализация знаний</i> (5 мин)	<p>Подводим к понятию «Интернет»: <i>Как узнать про все на свете?</i></p> <p><i>Ну конечно, в ИНТЕРНЕТЕ!</i> <i>Там музеи, книги, игры, Музыка, живые тигры!</i> <i>Можно все, друзья, найти В этой сказочной сети!</i></p> <p>Ребята, а для чего вам нужен Интернет?</p> <p>Ребята, кто может пользоваться сетью Интернет? С какой целью?</p> <p>Объявление темы урока. (1 слайд)</p>	<p>Слушают учителя, воспринимают предъявляемую информацию, анализируют ее и отвечают на вопрос загадки.</p> <p>-в интернете</p> <p>-Общение с друзьями, поиск информации, фильмы, игры и др.</p> <p>-Все у кого есть телефон или компьютер с доступом в Интернет.</p>	<i>Коммуникативные УУД:</i> развитие диалогической речи	Формы лично-ориентированного обучения, технологии проектной деятельности, дифференцированного обучения, обучения в сотрудничестве, игровые технологии.

	<p>Просмотр и обсуждение (2, 3 слайдов) Для чего вам нужен Интернет? Как вы считаете, есть ли какие-либо опасности при использовании сети Интернет? Что такое опасность?</p> <ul style="list-style-type: none"> - Что вы понимаете под угрозой? - Откуда может исходить угроза? <p>(просмотр 4 слайда — ролик об угрозах в сети Интернет), обсуждение увиденного</p> <ul style="list-style-type: none"> - Как вы понимаете, что значит быть безопасным в сети Интернет, что означает «безопасность»? - Как вы думаете, что такое «информационная угроза» и «информационная безопасность»? 	<p>Поиск информации, общение, учеба и т.д.</p> <p>-есть. Вирусы, мошенники и др. Да. Опасно это когда что-то угрожает. В интернете это вирусы, спам, мошенники и др.</p> <p>Угроза – запугивание, обещание причинить кому-нибудь неприятность, вред, зло.</p> <p>От взрослых, сверстников при личном общении, через мобильную связь, через ИНТЕРНЕТ.</p> <p>Беседа по содержанию просмотренного ролика. Выявление перечня опасностей, которые могут «ждать» в сети</p> <p>Безопасность — отсутствие каких-либо угроз. <i>Информационная угроза</i>- потенциальная возможность неправомерного или случайного воздействия на объект защиты,</p>		
--	---	---	--	--

		<p>приводящая к потере или разглашению информации. <i>Информационная безопасность детей</i> – отсутствие рисков, связанных с причинением информацией вреда здоровью и развитию детей.</p>		
<p><i>Объяснение нового материала (10 мин)</i> <i>Безопасность в сети wi-fi</i></p>	<p>Что такое Wi-Fi? Кто из вас пользовался данной сетью? Где вы ей пользовались? Как вы считаете сеть Wi-Fi в публичных местах безопасна или существуют угрозы? (слайд 6) Создает условия для выделения учениками информационных угроз.</p> <p>Wi-Fi далеко не безопасная сеть. Но что же делать? Как обезопасить себя и свои данные? (слайд 7)</p>	<p>Выделяют основные информационные угрозы.</p> <p>Ответы учеников: беспроводной интернет, пользовались дома и в общественных местах. Можно раздавать со своего смартфона.</p> <p>Изучение и разбор угроз Wi-Fi сети.</p> <p>Ответы учеников</p> <p>Выводы по изученной информации: использовать антивирус и брандмауэр, не передавать личную информацию по Wi-Fi, не вводить пароли, логины при использовании сети, отключить общий доступ к</p>	<p><i>Познавательные УУД:</i> извлечение необходимой информации из видеoinформации; структурирование знаний, рефлексия способов и условий действий</p> <p><i>Личностные УУД:</i> развитие логического мышления, знание основных моральных норм</p>	<p>Создание творческой атмосферы на уроке, включение учащихся в творческий процесс не только способствует развитию личности, но и снижает вероятность наступления утомления.</p>

		документам и папкам.		
Онлайн игры	<p>Кто из вас играл в игры на компьютере? Что такое сетевая игра?</p> <p>Какие опасности могут встретиться в играх? (слайд 8 — возможные угрозы в онлайн играх) Что же делать чтобы обезопасить себя, свои данные, аккаунт в сети? (слайд 9) Обсуждение, выводы</p>	<p>Ответы учеников: Игра в которой большое количество игроков, работает только в сети Интернет.</p> <p>Мошенники взламывают и крадут аккаунты, спам рассылки, вирусы, ложные сайты.</p> <p>Ответы: сложные пароли, никому не рассказывать свой логин и пароль и др.</p> <p>Изучают советы по безопасности аккаунта, делают выводы.</p>		
Кибербуллинг	<p>В настоящее время часто встречается понятие «Кибербуллинг». Знаете ли вы, что оно означает? Да. (слайд 10) Это виртуальные издевательства в сети.</p> <p>(слайд 11, 12) И таких издевательств существует большое количество. Разберем основные из них: Флейм — перепалка. Атаки. Буллинг по сотовой связи.</p>	<p>Ответы: издевательства в сети.</p> <p>Изучают информацию, выделяют основные виды кибербуллинга. Предлагают варианты действий в случае возникновения данного вида угроз.</p>		

	<p>Клевета. Самозванство. Изоляция. Киберпресследование.</p>	<p>Выводы учеников.</p>		
<p>Компьютерные вирусы</p>	<p><i>(экран компьютера гаснет)</i> <i>Экран компьютера погас,</i> <i>И на экране вырос</i> <i>Какой-то шарик с парой</i> <i>глаз</i> <i>И надписью: "Я - вирус! "</i> <i>Стал прыгать и</i> <i>кривляться</i> <i>И мне в лицо смеяться: "Я</i> <i>победил. Компьютер мой!</i> <i>Никто не справится со</i> <i>мною! "</i> <p>Встречались ли вы с компьютерными вирусами? И что же нам теперь делать? (слайд 13) Изучение и обсуждение методов защиты компьютера от вредоносных программ.</p> </p>	<p>Ответы детей: нам поможет антивирус, обновление ПО.</p> <p>Изучают информацию, выделяют основные методы защиты от вредоносного ПО.</p>		
<p>Секстинг</p>	<p><i>Еще одна угроза которая встречается в сети — секстинг — пересылка личных фотографий.</i> (слайд 14) <i>Изучение, обсуждение.</i> <i>Выводы.</i></p>	<p>Изучают информацию, выделяют основные советы по размещению личных фото в сети Интернет и мерах их защиты.</p>		
<p>Физкультминутка (1 мин)</p>	<p><i>Мы все вместе улыбнемся,</i></p>	<p>Выполняют физминутку под руководством учителя</p>		<p>Релаксационная двигательная</p>

	<p><i>Подмигнем слегка друг другу, Вправо, влево повернемся И кивнем затем по кругу. Все идеи победили, Вверх взметнулись наши руки. Груз забот с себя стряхнули И продолжим путь науки.</i></p>			<p>активность, направленная на преодоление устомления (физминутка, гимнастика для глаз)</p>
<p><i>Социальные сети</i></p>	<p><i>У меня среди друзей Есть барсук и соловей Еж, кукушка и енот Африканский бегемот Заяц, серый волк, питон Даже есть Индийский слон Все выкладывают фото Вот кулик свое болото Волк - луну, тушканчик - норку Мышь-полевка - хлеба корку За порядком здесь медведь! Тихо наблюдает Как зовется эта сеть, Может кто-то знает?</i></p> <p>Кто знает, что есть в социальной сети? Кто уже пользовался ей? - Какие вы знаете социальные сети?</p>	<p>Социальная сеть</p> <p>Участвуют в обсуждении, отвечают на вопросы.</p> <p>Предполагаемые ответы:</p>		

	<p>- Кто уже зарегистрирован в этих сетях? В социальных сетях можно встретить опасности, хулиганов. Почему? Чтобы избежать этого, нужно обозначить правила безопасного использования Интернета. Организует обсуждение, объясняя новый материал. (слайд 15 - видеоролик)</p>	<p>Интернет, социальные сети Сайты, созданные для объединения людей по определенному признаку или интересу, социальные взаимоотношения в Интернете. Просмотр ролика. Вывод о безопасном использовании социальных сетей.</p>		
Фишинг	<p>Следующая угроза с которой мы знакомимся — фишинг (слайд 16) — это кража личных данных. (слайд 17)</p>	<p>Изучают материал. Предлагают способы борьбы с фишингом.</p>		
Электронная почта	<p><i>Собака, мыло, точка, ру - Как быстро ходит почта! Сейчас лишь кнопку нажму, И ты читаешь строчки.</i> Что вы знаете об электронной почте? У кого из вас есть своя ЭП? Что нужно для создания почтового ящика? (слайд 18) Изучение, выводы</p>	<p>Ответы учеников. Быстрая передача данных — письма, фото, аудио и другой информации. Выбор почтового сервера и регистрация. Изучение, выводы</p>		
Электронные деньги	<p>В современном мире</p>			

	широко используются Электронные деньги. Знакомы ли вы с ними? Банковские карты для детей сейчас могут выпускаться с 6-7 летнего возраста. С одной стороны это удобно, но с другой вы должны уметь правильно пользоваться ими. Какие правила необходимо соблюдать? (слайд 19)	Ответы учеников. Ответы учеников: надежно хранить, не сообщать пароль от карты, не вводить данные на неизвестные сайты. Изучение информации, выводы по безопасности.		
Пароль	Безопасный пароль — защитит ваши данные. (Изучение слайдов 20, 21)	Выводы учеников о надежности их паролей от различных аккаунтов, социальных сетей и банковских карт.		
<i>Первичное закрепление знаний</i>	Проведение теста на закрепление полученных знаний. (приложение 1)	Самостоятельное выполнение теста.	<i>Личностные УУД:</i> развитие логического мышления. <i>Познавательные УУД:</i> структурирование знаний, рефлексия способов и условий действий, контроль и оценка процесса и результатов деятельности.	Включение в содержательную часть урока вопросов, связанных со здоровьем и здоровым образом жизни.
<i>Подведение итогов урока. Рефлексия (3 мин)</i>	Подводит итог урока. Обеспечивает рефлексивную	Оценивают урок. Воспринимают информацию. Фиксируют выводы.	<i>Коммуникативные УУД:</i> построение речевого высказывания	Формы личностно- ориентированного обучения, технологии

	<p>деятельность учащихся. Оценивает работу учащихся.</p> <p>Вопросы: - Какие правила нужно соблюдать в Интернете? - Что из себя представляет Интернет? - Можно ли доверять любой информации, полученной из Интернета? - Как защитить компьютер при работе в Интернете? - Был ли урок полезным для тебя?</p> <p>Раздает памятки и кратко поясняет информацию в памятках.</p>	<p>Отвечают на вопросы учителя</p>	<p>в устной форме.</p> <p><i>Личностные:</i> контроль и оценка процесса и результатов деятельности</p>	<p>проектной деятельности, дифференцированного обучения, обучения в сотрудничестве, игровые технологии.</p>
--	---	------------------------------------	--	---

Тест на тему: «Безопасность в социальных сетях»

1. Что такое Интернет?

- а) вычислительная сеть
- б) всемирная сеть
- в) компьютерная игра

2. Нужно ли в интернете всем сообщать свою фамилию, имя, адрес, номер школы?

- а) всем виртуальным друзьям нужно рассказать о себе
- б) никогда не сообщать личную информацию
- в) сообщать только вымышленную информацию

3. Можно ли отправлять SMS или оставлять свой номер телефона с незнакомого сайта, чтобы получить код доступа к игре или подарку?

- а) никогда не следует отправлять SMS или давать свой номер телефона
- б) всегда оставлять номер телефона, а SMS слать нельзя
- в) всегда отправлять сообщение и давать номер, чтобы получить код доступа

4. Виртуальный друг предлагает встретиться, ваши действия:

- а) встретиться с виртуальным другом в торговом центре
- б) сообщить родителям о встрече
- в) встретиться с виртуальным другом в заброшенном, таинственном месте

5. На вашу электронную почту пришло письмо от неизвестного адресата, вы:

- а) сохраните в черновики и откроете позднее
- б) откроете немедленно
- в) никогда не открываете писем от неизвестных адресатов

6. В сети вы встретились с дразнилками и оскорблениями, вы:

- а) отвечаете грубостью
- б) заблокируете этого человека и сообщите родителям
- в) никому об этом не говорите

7. Антивирусная программа - ...

а) программа обнаружения вирусов на вашем компьютере

б) название журнала о компьютерах

в) программа закаливания организма

8. Сколько времени детям, по мнению специалистов, можно проводить за компьютером?

а) пока не выиграешь в любимую игрушку

б) пока не подготовишься к урокам

в) не более часа в день

Ключи к тесту:

1.б

2.б

3.а

4.б

5.в

6.б

7.а

8.в

Безопасное общение в интернете

Защищайте свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату рождения и другую личную информацию.

Ограничьте список друзей. В друзьях не должно быть случайных и незнакомых людей.

При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.

При общении с незнакомыми людьми, не используйте свое реальное имя и другую личную информацию: имя, место жительства, место учебы и прочее.

Защищайте свою репутацию – держите ее в чистоте. Подумайте, прежде чем что-то опубликовать, написать и загрузить.

Для социальной сети, почты и других сайтов используйте разные пароли.

Избегайте размещения фотографий в интернете, где вы изображены на местности, по которой можно определить ваше местоположение.



ПАМЯТКА

Как распознать фишинговую страницу

Присмотрись!

1. В названии сайта или в домене есть ошибка или опечатка.
2. Используются неверные цвета или изображения логотипа.
3. Наличие грамматических и орфографических ошибок в тексте страниц.
4. Большинство кнопок на страницах не работают.
5. Протокол шифрования для передачи данных пользователей начинается на «https://».

Действуй!

1. Установи защитное решение, оно не даст перейти по фишинговой ссылке.
2. Скрой личные данные (номер телефона и др.) из описания профиля.
3. Установи сложный пароль!
4. Включи дополнительный уровень безопасности – двухфакторную аутентификацию!
5. Сделай страницу приватной!

ПАМЯТКА

Как обезопасить свой смартфон от вредоносных программ и потери данных?

1. В настройках телефона запретить установку приложений из внешних источников;
2. регулярно обновлять операционную систему;
3. установить антивирус;
4. не скачивать приложения с подозрительных сайтов.