Конкурсный урок

Класс 8

Тема «Общие принципы безопасности в цифровой среде

Структура урока

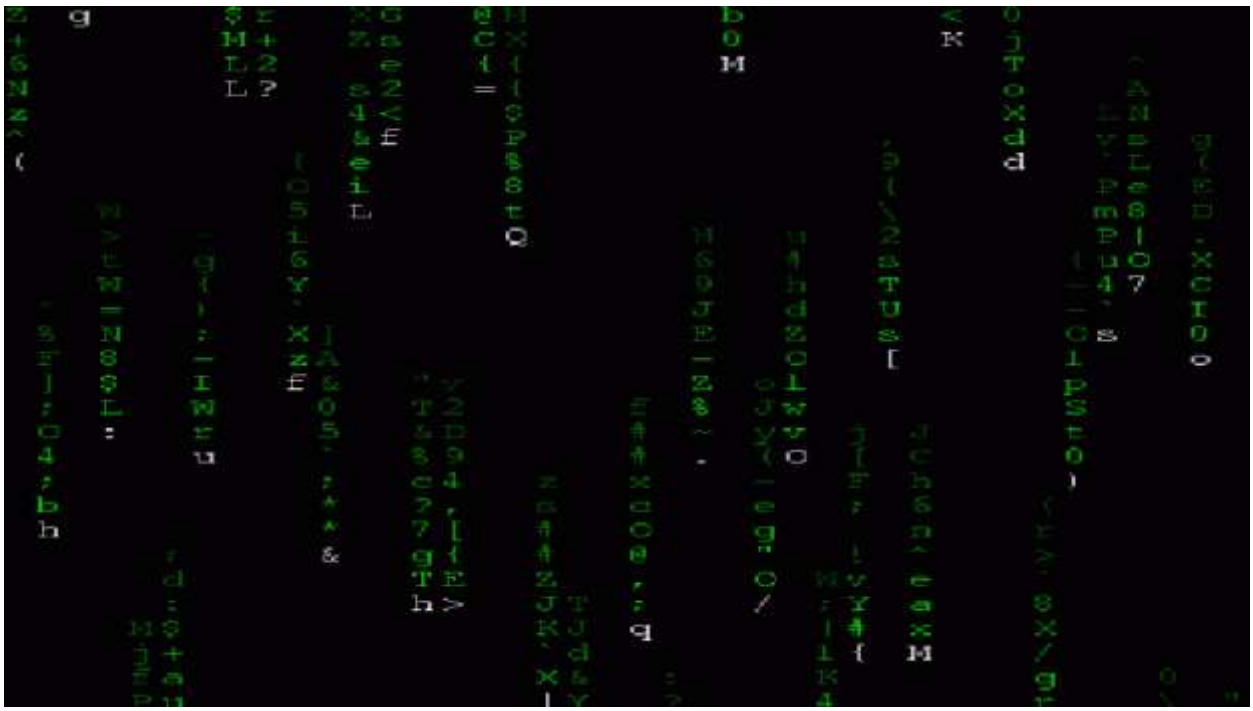
1 Введение

Добрый день ребята. Меня зовут Буйновский Александр Андреевич, я учитель ОБЖ из школы 83 города Северска. Сегодня я проведу с вами урок ОБЖ по новой теме.

2. подводка к теме урока

Для того, чтобы понять, о чем именно мы с вами сегодня будем изучать и познавать в рамках ОБЖ я дам вам подсказку. Квест. Вопрос – можно назвать это по-разному.

Выводим гиф с Матрицей



Знаете ли вы, откуда это изображение?

С чем оно связано?

(ответы детей - \матрица, виртуальный мир, связанный с реальностью но в компьютере и т.д. Подводим их к мысли, что безопасность важна не только в реальности)

3 Постановка темы урока

Действительно, мы с вами живем, работаем, учимся или играем, отдыхаем не только в реальном мире, но и в цифровой среде. Но правила безопасности нужно знать и следовать им постоянно, даже в виртуале. А для этого нужно понимать, что такое цифровая среда и чем она может быть опасна для пользователя.

В рабочей тетради записываем дату – 16/17 апреля.

Тема - Общие принципы безопасности в цифровой среде

Сегодня мы с вами обсудим что такое цифровая среда, основные виды опасностей цифровой среды и базовые принципы безопасности при работе в цифровой среде

Мы пользуемся различными устройствами – гаджетами, которые дают нам право доступа в цифровую среду. Приведите пример, как Вы используете гаджеты, с какой целью, для чего?

(ответы детей - ***социальные сети и форумы, мессенджеры, компьютерные игры, мобильные приложения, электронные почтовые сервисы, видеохостинги и т. д***.)

Спасибо за ответы. Таким образом, мы сами создаем для себя цифровую среду. Она виртуальна, но через нее можно совершать действия и влиять на то, что происходит в реальности.

Давайте с вами запишем определение в тетради: (выводим на экран)

Цифровая среда — пространство, доступ в которое осуществляется посредством электронных устройств и в котором с помощью программных средств происходит активное взаимодействие людей между собой или людей с электронными сервисами.

Цифровой характер среды означает, что весь контент (сообщения, комментарии, фотографии и т.д.) оцифрован, а значит, доступен для обработки, систематизации и анализа (как с помощью специального программного обеспечения, так и вручную). Кроме того, будучи размещён на платформах и в хранилищах в Интернете, он хранится вечно, а это значит, что в любой момент информация о любом пользователе может быть обнаружена и применена с той или иной целью.

Давайте попробуем выделить особенности цифровой среды, выведенные на экран, обсудим их и запишем в тетрадь.

Задача – объяснить, чем именно эти особенности отличают виртуальную среду от реальной (**ВЫВОДИМ НА ЭКРАН ТОЛЬКО ОСОБЕННОСТИ, без определения**):

1. **«Анонимность»** - не человек, а аккаунт или профиль - снижает у некоторых людей степень ответственности за свои поступки и вызывает желание нарушить правила поведения и этические нормы, которые в реальной жизни они, как правило, соблюдают
2. **Иллюзия приватности** - необоснованная уверенность пользователя в том, что он полностью контролирует размещённую в цифровом пространстве им самим информацию, включая персональную. Сведениями личного характера могут воспользоваться злоумышленники в корыстных целях.
3. **Вредоносное ПО** - угроза заражения цифровых устройств вредоносными программами, которые могут вывести технику из строя или привести к потере пользователем важных для него данных
4. **Противоправные действия** людей (взлом аккаунта, спам, фишинг и другие виды мошенничества в цифровой среде) О них более подробно будет рассказано на следующем уроке по ФОП.

Таким образом, об обеспечении безопасности в цифровой среде заботятся как на индивидуальном, так и на общественном и государственном уровнях: принимаются специальные цифровые законы, выпускаются антивирусные программы, владельцы социальных сетей разрабатывают и регулярно обновляют правила поведения в них. Но эти меры не могут гарантировать полной защищённости в цифровой среде, и каждый пользователь должен лично принимать участие в обеспечении собственной безопасности. Для защиты от каждого вида опасности разработаны свои приёмы, а если избежать её не удалось, применяются специальные механизмы/алгоритмы решения проблемы.

Основные опасности цифровой среды

Мозговой штурм – перечислить, чем опасна может быть цифровая среда

Записи делаем на доске мелом / маркером

А сейчас мы с вами будем перечислять опасности, которые могут возникнуть в цифровой среде для человека, слабо разбирающегося в правилах безопасности. Работать будем при помощи «мозгового штурма». Кто не в курсе, что это такое? Рассказываю – у нас есть вопрос, и мы фиксируем первое, что приходит нам в голову по этой теме. Фиксируем все, даже те идеи и мысли, которые могут показаться не совсем нормальными или невыполнимыми. Приведу пример, не связанный с ОБЖ, но доказывающий, что иногда незнание дает толчок к развитию

РАССКАЗ: В 1939 году Джордж Бернард Данциг, докторант в Калифорнийском университете, Беркли, опоздал на лекцию по статистике и увидел на доске две задачи. Они были примерами нерешённых проблем статистики, а он счёл их домашним заданием – записал и решил. Уравнения, с которыми справился Данциг, скорее не нерешаемые задачи, а недоказанные статистические теоремы, для которых он нашёл доказательства.

А теперь давайте запишем то, что сформировало наше мышление по поставленному вопросу:

Дети перечисляют: мошенничество, опасная информация, буллинг, взлом данных, воровство денег, обман, некачественный товар, вербовка, игромания. Фейковые новости и др.).

Обобщая вышесказанное, можно выделить 4 основных группы рисков, связанных с цифровой средой:

Выводим на экран

Выделяют 4 видов рисков:

- **Коммуникационные риски**
- **Контентные риски**
- **Потребительские риски**
- **Технические риски**

Делаем записи в тетради с 4мя группами рисков, проговаривая, о чем именно они.

Опасности и риски мы с вами обсудили, осталось понять, как этого избежать. Давайте ответим на следующий вопрос.

Существуют ли правила безопасного поведения в Интернете (ответы детей)

Работа со «стикерами» 4х цветов. Дать право выбрать себе цвет. Каждый цвет – определенный «риск»

Каждый из вас выбрал себе стикер определенного цвета. На нем нужно будет записать кратко одно правило безопасности, чтобы избежать одной группы рисков цифровой среды. постарайтесь записать кратко в 2-4 слова, понятным почерком, потому что эти записи придется потом прочитать и объяснить.

Красные стикеры – потребительские риски

Желтые стикеры – коммуникационные риски

Зеленые – контентные риски

Белые – технические риски

Дети придумывают правила безопасности, размещают их на экране / доске по группам рисков. Выходят по очереди, зачитывают правило и прикрепляют их к «своим» рискам

Подводим итог. Таким образом, мы с вами сделали «сборник» правил безопасного поведения в сети – в цифровой среде. Правила довольно простые, но действенные, если их соблюдать. Вы уже много знаете по этому вопросу, но среди ваших родных могут быть люди, которые слабо разбираются в вопросах безопасности, тем более в цифровой среде. Младшие братья и сестры, или наоборот – бабушки и дедушки (прабабушки и прадедушки) – для них Вы можете стать наставником по безопасности в цифровой среде.

Опрос МИМИО

Тест – для получения оценки за урок:

5 вопросов выводим на экран. Объясняем, что такое МИМИО и как оно работает. Проводим тестирование. Объясняем – 5 ответов = 5, 4=4, 3=3 и т.д. Бонусы за устный ответ учитываются при подведении итогов урока.

Записываем домашнее задание:

1. Повторить материалы урока : цифровая среда, риски цифровой среды, правила безопасного поведения в сети.
2. Подготовить сообщение о том, что такое цифровая и игровая зависимость, их симптомы и особенности поведения человека с таким диагнозом.

На память о нашем уроке и для закрепления правил безопасного поведения в цифровой среде хотел бы вам выдать для ознакомления и использования буклеты по информационной безопасности (выдача буклетов). До свидания всем