**Сценарий Урока Цифры**

**Учитель: Мисюра Т.К., учитель информатики**

**Ход урока**

**Слайд 1**

Вводная часть: Приветствие, демонстрация сайта «Урока цифры». Организационный момент (проверка присутствующих) – (3 минут)

«Здравствуйте, сегодня у нас будет с одной стороны не совсем обычный урок, но с другой, хорошо вам знакомый. Так как мы регулярно знакомимся с мероприятиями, которые нам предлагают организаторы и партнеры проекта «Урок цифры», такие как: Фирма «1С», Яндекс, Лаборатории Касперского, а также Академия искусственного интеллекта благотворительного фонда Сбербанка «Вклад в будущее». Сам же проект стартовал в декабре 2008 года и как мы видим, становиться все более популярным и актуальным.

На наш урок сегодня пришли гости, которым вы можете задать интересующие вас вопросы

**Слайд 2.**

Представление гостей

Спасибо за заданные вопросы и конечно интересные и познавательные ответы.

**Слайд 3**

## Как-то просматривая материалы о безопасности в сети интернет, я натолкнулась на блог Касперского, в частности на статью Александра Родченко [Артефакты в CLR: как маскируют современные кибератаки и как SOC может их обнаружить](https://habr.com/ru/company/kaspersky/blog/648149/). В этой статье автор раскрывает причину, почему атакующие предпочитают использовать старые утилиты, а не писать новые, где (а на самом деле — когда) в CLR появляются артефакты от «старых добрых» утилит, и как ваш SOC может вовремя их задетектить(обнаружить).

**Слайд 4**

**(Аналитик** **SOC** (Security Operations Center Monitoring) является частью команды Kaspersky Lab **SOC**, которая занимается непрерывным мониторингом безопасности, облегченным реагированием на инциденты и выявлением киберугроз

**SOC** (security operations center) – центр управления информационной безопасностью. Основными задачами SOC является осуществление мероприятий по мониторингу и реагированию на инциденты ИБ.

https://ria.ru/20210908/kiberataki-1749149024.html

Может в не далеком будущем мы начнем читать коды, как детектив, следя за ходами злоумышленников - хакеров и получать эстетическое удовольствие от раскрытия их злостных преступлений. Предполагаю, это будут очень большие тома.

**Слайд 5**

Ведь все чаще и чаще мы в своей жизни обращаемся в интернет к цифровым системам, которые стали для нас незаменимыми помощниками. Например, заказать продукты, купить билеты, записаться к врачу и многое другое. И везде мы оставляем свои данные. А всегда ли это безопасно?

Ответ детей….

Вспомните, как часто мы слышим из разных информационных источников слова – мошенники, хакеры, взломы, атаки. Да и мы с вами недавно столкнулись с такой проблемой, я имею ввиду сетевой город. Наши волнения были обоснованы, ведь именно наши данные хранились в базах, хорошо, что есть отличные специалисты. Приведу еще примеры самых громких кибервзломов и утечек в России за 2021год.

**Слайд 6**

Давайте посмотрим мотивы злоумышленников

Гистограмма. Выводы.

**Хактивизм** — **это** уникальная смесь слов «хакерство» и «активизм», которая появилась, когда люди используют Интернет для демонстрации по политическим или социальным причинам.

**Слайд 7**

Как вы, наверное, уже поняли тема нашего урока действительно актуальна как никогда. И тема нашего урока…?

Ответ детей….

Сегодня вы познакомитесь с понятием “кибератака”, узнаете, как специалистам по информационной безопасности удается обнаруживать кибератаки, исследовать их и понять, какая группа злоумышленников может за ними стоять.

**Слайд 8**

Поэтому Урок цифры» предлагает погрузиться в увлекательную визуальную новеллу-комикс, сюжет которой строится вокруг исследования кибератаки, совершенной на банк. Сюжет истории основан на [реальных событиях](https://youtu.be/MV1ILcoUG64), которые происходили в разных странах мира! Главный герой — кибердетектив Мидори Кума помогает исследовать случившийся инцидент. Попутно он рассказывает про работу специалистов по информационной безопасности, учит отличать фишинговые письма от обычных, объясняет, почему важно обновлять программное обеспечение. Но сначала давайте посмотрим видеолекцию от эксперта «Лаборатории Касперского» по кибербезопасности.

**Слайд 9**

*Видеолекция*

Совместный просмотр видеолекции (8 минут) с комментариями и обсуждением во время пауз.

**Слайд 10**

Из видеолекции мы узнали кто такие эксперты по кибербезопасности, а также что такое кибератака. Давайте еще раз это проговорим.

**Слайд 11**

Опрос после просмотра видеолекции

* Какие три уровня кибератак можно выделить?
* 90% — это массовые киберугрозы, с помощью которых злоумышленники обманываю людей?
* Как защитить себя от киберугроз?

**Слайд 12**

Досматриваем ролик.

**Физминутка**

Прохождение тренажера

**Слайд 13**  Рефлексия.

Вопросы

1. Что вам больше всего запомнилось?

2. Кто прошел все задания?

3. Какое задание показалось вам самым интересным?»

**Слайд 14**

* На этом занятии мы освоили…
* Сегодня мы научились…
* Мне было сложно…
* Я понял, что….я планирую….

**Слайд 15**

И в заключение хочу добавить оптимизма и позитива словами Евгения Касперского

«Я твёрдо уверен, что само понятие «кибербезопасность» в скором времени себя изживет, а на замену ему придёт концепция «кибериммунитета».