# Летний интенсив «Марс атакует!» Порядок действий ликвидации последствий сбоев системы, кибератак

## Возможные пути решения проблемы

# Темы для исследований

«Синий экран. (англ. Blue Screen of Death, Blue Screen of Doom, BSoD) — название сообщения о критической системной ошибке в операционных системах Microsoft Windows»

«Код ошибки»

«Взлом и кибератака. Как не стать жертвой хакера»

«Вредоносное ПО – способы распространения и защиты»

# Что должно быть в презентации

- оглавление презентации
- определение темы и периода исследований
- ситуации, в которых упоминается тема исследований в СМИ, и основные инфоповоды, связанные с темой (с указанием дат)
- скриншоты наиболее интересных и показательных сообщений в СМИ
- наиболее популярные и наиболее, по вашему мнению, достоверный источники информации на выбранную тему (список);
- рекомендации как избежать данной ситуации (не менее 4).

# Описание проблемной ситуации

О чем говорит это сообщение?
Сталкивались ли вы с подобными сообщениями или им подобными? Если да, с какими именно и как вы себя вели?
Что бы сделали Вы, получив такое сообщение?
Какой ущерб это может принести?

- Программные сбои и сопровождающие их оповещения очень редко, когда становятся популярными и узнаваемыми среди пользователей.
- Культовый статус обычно получают или наиболее распространённые ошибки (например, знаменитейшая «404-ая»), или наиболее значимые.
- Среди последнего типа безусловным лидером принято считать «синий экран смерти». Многими владельцами систем Windows встреча с этим явлением до сих пор отчетливо помнится. Появление на экране злополучных надписей на английском было предвестником или дорогостоящего ремонта в сервисном центре, или не менее дешевого приобретения комплектующих.

# Теоретический блок

Эта ошибка возникает всякий раз, когда Windows обнаруживает сбой программного обеспечения, аппаратных средств или ошибку драйвера, которые не позволяют ему правильно продолжать свою работоспособность.

История синего экрана и почему он появляется

https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BD%D0%B8%D0%B9_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD_%D1%81%D0%BC%D0%B5%D1%80%D1%82%D0%B8

- Что можно сделать если появилось данное сообщение?
- Что можно сделать, чтобы избежать появления данного сообщения?

Вопросы:

Как часто возникает такая проблема?

Каковы причины отображения данного сообщения на экране?

Что предлагают предпринять?

Стоит ли доверять тому, что пишут в сети? Как проверить?

Действительно ли сбой в системе или это вирус?

Статья о причинах появления и способах решения

Вопросы:

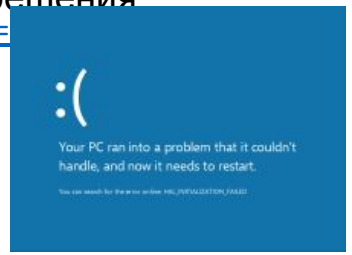
- Какие поисковые системы будем использовать?
- Какие источники?
- Каким источникам будем доверять?
- Какие поисковые запросы создаем?

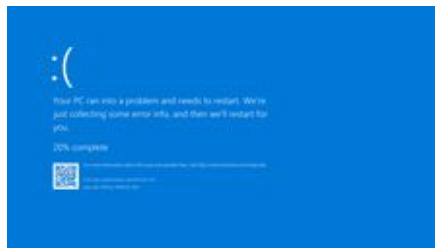
Подведение итогов исследования

- В какой степени можно доверять ответам в социальных сетях?
- Что еще следует изучить, чтобы разобраться в данной тематике?
- Каков план действий, при обнаружении данного сообщения на экране монитора?

Задание до четверга

Составление плана действий (пошаговой инструкции) по решению данной проблемы. Может быть сделано в любом удобном виде.





# Изучение фейковых сообщений и вредоносного ПО в сети Интернет

- В связи с тем, что большинство контента является платным – таким как музыка, фильмы и книги, большинству пользователей приходит в голову мысль о получении его путями, не совсем законными.
- Это можно сделать через сайты файлообменники, торрент-трекеры или сайты сомнительного характера, которые напрямую предлагают подобные услуги.
- Результат может быть весьма плачевным, если после этого на вашем компьютере появится вредоносное программное обеспечение. Оно может быть достаточно безобидным, а может привести и к весьма серьёзным последствиям.

# Изучение фейковых сообщений и вредоносного ПО в сети Интернет

Компью́терный ви́рус — вид вредоносного программного обеспечения, способного внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

- Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов и даже удаление операционной системы, приведение в негодность структур размещения данных, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

В обиходе «вирусами» называют всё вредоносное ПО, хотя на самом деле это лишь один его вид.

https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81

- https://www.kaspersky.ru/resource-center/threats/viruses-worms Касперский о компьютерных вирусах

С какими компьютерными вирусами Вы встречались? Знаете их названия?

- https://technomode.ru/article/2018/05/04/samye-gromkie-kompyuternye-virusy-za-god - Статья про Самые «громкие» компьютерные вирусы за 2018 год

Какие виды «Вредоносного ПО» Вы еще знаете?

- https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs - Методы и признаки заражения ПО
- http://www.syzran-soft.ru/?page_id=42

Это может быть интересно https://www.comss.ru/page.php?id=2853