

СЕТЬ ЦЕНТРОВ ЦИФРОВОГО  
ОБРАЗОВАНИЯ ДЕТЕЙ «ИТ-КУБ»  
ИТ-CUBE.Смоленск

ГРУППА

КБ-1

## Кейс 2:

# ПОРЯДОК ДЕЙСТВИЙ ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СБОЕВ СИСТЕМЫ, КИБЕРАТАК. ВОЗМОЖНЫЕ ПУТИ РЕШЕНИЯ ПРОБЛЕМЫ

## Занятие 2

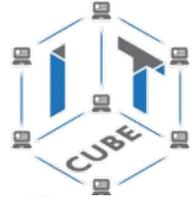


**ИЗУЧЕНИЕ ФЕЙКОВЫХ СООБЩЕНИЙ И ВРЕДОНОСНОГО ПО В СЕТИ ИНТЕРНЕТ И С ПОМОЩЬЮ СИСТЕМЫ «КРИБРУМ». СПОСОБЫ РАСПРОСТРАНЕНИЯ И ЗАРАЖЕНИЯ. ИЗУЧЕНИЕ ДЕЙСТВИЙ ПРИ СТОЛКНОВЕНИИ с ВИРУСОМ.**

ПРЕЗЕНТАЦИЮ РАЗРАБОТАЛ НАСТАВНИК :  
– ЕСИПЕНКО ВЛАДИМИР МИХАЙЛОВИЧ

**Кибергигиена и работа с большими данными/наставник Есипенко В.М.**

Понятие сбоя системы и синего экрана. Способы восстановления системы.  
Постановка задачи исследования. Изучение сообщений о синем экране.



*Домашнее задание*

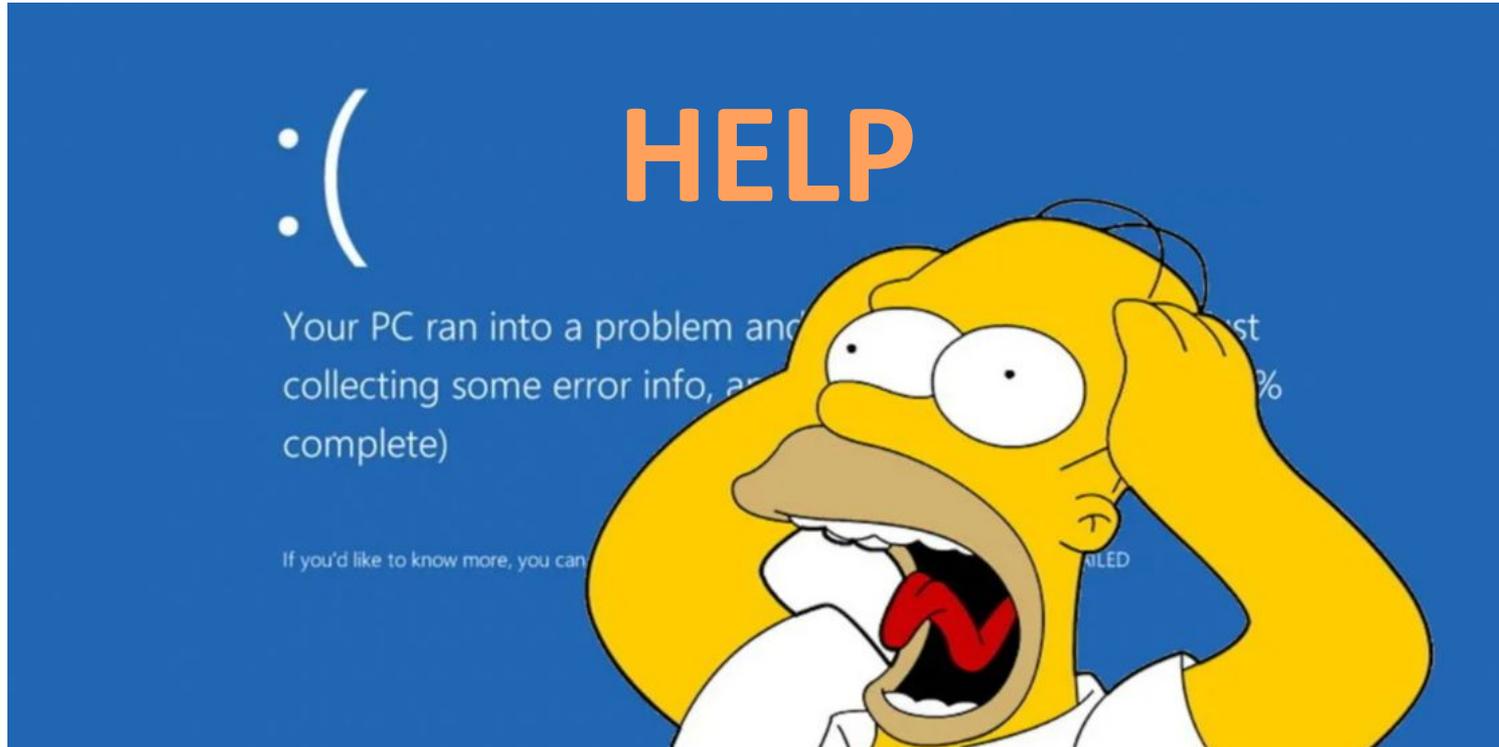
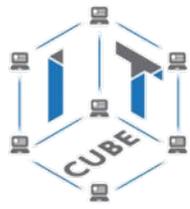
Кейс 2. Занятие 1

# СОСТАВИТЬ И ПРЕДСТАВИТЬ ПЛАН ДЕЙСТВИЙ (ПОШАГОВОЙ ИНСТРУКЦИИ) ПО РЕШЕНИЮ ПРОБЛЕМЫ «СИНЕГО ЭКРАНА» ИЛИ СООБЩЕНИЯ О НЕПОЛАДКАХ.

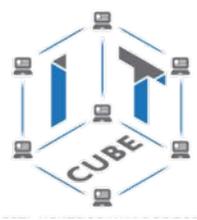
Может быть  
сделано  
в  
любом удобном  
ВИДЕО



**Понятие сбоя системы и синего экрана. Способы восстановления системы.  
Постановка задачи исследования. Изучение сообщений о синем экране.**



Понятие сбоя системы и синего экрана. Способы восстановления системы.  
Постановка задачи исследования. Изучение сообщений о синем экране.



## Синий экран смерти (*Blue Screen of Death, Blue Screen of Doom, BSoD*)

- 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?

**СМОТРИМ В СИСТЕМЕ КРИБРУМ И ПОИСКОВЫХ**

Понятие сбоя системы и синего экрана. Способы восстановления системы.  
Постановка задачи исследования. Изучение сообщений о синем экране.

# СОСТАВЛЕНИЕ И ПРЕДСТАВЛЕНИЕ ПЛАНА ДЕЙСТВИЙ (ПОШАГОВОЙ ИНСТРУКЦИИ) ПО РЕШЕНИЮ ДАННОЙ ПРОБЛЕМЫ.



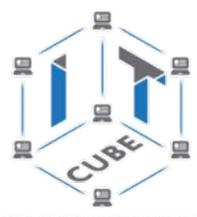
**Понятие сбоя системы и синего экрана. Способы восстановления системы.  
Постановка задачи исследования. Изучение сообщений о синем экране.**

---



**my.kribrum.ru**

<b>Кванториум - вводный (дети, кейс 2)</b>	
<b>ЛОГИН</b>	<b>пароль</b>
<b>Kv720_EsipenkoV_d2</b>	<b>MrRXUBLrMK</b>



## ИНТЕРНЕТ КОНТЕНТ



ЧАЩЕ ПЛАТНЫЙ

ФАЙЛООБМЕННИК И, ТОРРЕНТ-ТРЕКЕРЫ



РИСКИ ЗАРАЖЕНИЯ



```
A problem has been detected and windows has been shutdown to prevent damage to your computer.
DRIVER_IRQL_NOT_EQUAL
If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow
these steps:
Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or
software manufacturer for any windows updates you might need.
If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as
caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to
select Advanced Startup Options, and then select Safe Mode.
Technical information:
*** STOP: 0x0001 (0x00C,0x002,0x00,0xF8685A89)
*** gv3.sys - Address F8685A89 base at F8685000, DateStamp 3dd9919eb
Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further assistance.
```



## Синий экран смерти (Blue Screen of Death, Blue Screen of Doom, BSoD)

A problem has been detected and Windows has been shut down to prevent damage to your computer.

**PROCESS\_INITIALIZATION\_FAILED** **Название**

If this is the first time you've seen this Stop error screen, restart your computer, If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information **Код**

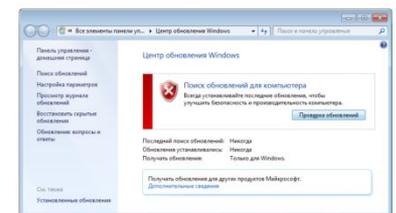
\*\*\* STOP: **0x00000060** (0xF2N094C2, 0x00000001, 0x4FQ1CCC7, 0x00000000)

\*\*\* **4FQ.sys** - Address FWTV1999 base at 4S4M5000, Datestamp 4d5dd88c

**Сбойный файл**  
Begin by checking physical memory  
Physical memory dump complete  
Contact your system administrator or technical support for further assistance.



Обновление системы и драйверов



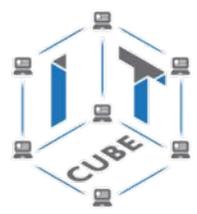
Щит от вирусов и угроз

Защита устройства от угроз.

Текущие угрозы

Текущих угроз нет.  
Последнее сканирование: 04.10.2015 11:06 (полное сканирование)  
Найдены угрозы (0).  
Проверка длилась 1 ч 21 мин  
Проверено файлов: 831806.

Быстрая проверка

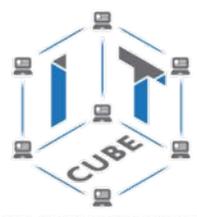


## ИЗУЧЕНИЕ ФЕЙКОВЫХ СООБЩЕНИЙ И ВРЕДНОСНОГО ПО В СЕТИ ИНТЕРНЕТ



### DRIVER IRQ NOT LESS OR EQUAL

- Вариант 1. Удаляем конфликтующий драйвер
- Вариант 2. Удаляем программу, использующую конфликтующий драйвер
- Вариант 3 Обновляем драйвера сетевых, аудио и видео карт
- Вариант 4. Отключаем внешние устройства
- Вариант 5. Используем возможности Msinfo32.exe
- Вариант 6. Ищем вируса
- Вариант 7. Устраняем ошибки реестра
- Вариант 8. Проверяем стабильность работы системных файлов
- Вариант 9. Установите все доступные обновления Windows
- Вариант 10. Используйте восстановление системы
- Вариант 11. Проверьте винчестер и планки памяти на работоспособность



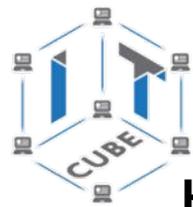
# ИЗУЧЕНИЕ ФЕЙКОВЫХ СООБЩЕНИЙ И ВРЕДНОСНОГО ПО В СЕТИ ИНТЕРНЕТ



## •КАК ВЫ ДУМАЕТЕ КАКИЕ СУЩЕСТВУЮТ КАНАЛЫ РАСПРОСТРАНЕНИЯ ВИРУСА?



>> Флешки, электронная почта, системы обмена мгновенными сообщениями, веб-страницы, Интернет, локальные сети



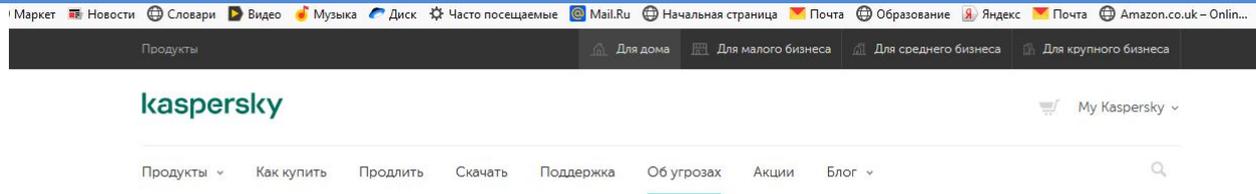
# ИЗУЧЕНИЕ ФЕЙКОВЫХ СООБЩЕНИЙ И ВРЕДОНОСНОГО ПО В СЕТИ ИНТЕРНЕТ



## КОМПЬЮТЕРНЫЙ ВИРУС

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

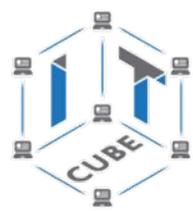
<https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>



Главная > Для дома > Об угрозах > Угрозы

## Компьютерные вирусы и вредоносное ПО: факты и часто задаваемые вопросы





## ИЗУЧЕНИЕ ФЕЙКОВЫХ СООБЩЕНИЙ И ВРЕДНОСНОГО ПО В СЕТИ ИНТЕРНЕТ



# РАБОТА В ГРУППАХ

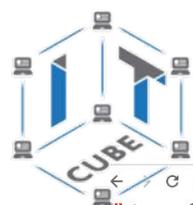
Задачи:

1. Анализ временной динамики сообщений, какова сейчас ситуация в данной проблеме (Пик/ подъем/спад)
2. Популярные авторы, в каких источниках происходит наибольшее упоминание.
3. Что посоветовать сделать при данной проблеме?



**my.kribrum.ru**

<b>Кванториум - вводный (дети, кейс 2)</b>	
<b>ЛОГИН</b>	<b>пароль</b>
<b>Kv720_EsipenkoV_d2</b>	<b>MrRXUBLrMK</b>



# ИЗУЧЕНИЕ ФЕЙКОВЫХ СООБЩЕНИЙ И ВРЕДОНОСНОГО ПО В СЕТИ ИНТЕРНЕТ



КРИБРУМ  
Мы слушаем сеть

my.kribrum.ru/documents#fpage\_opts=1\_123&author\_age=&author\_birthday=&calendar=month&from\_objects=9151315480038133329%2C9151315480037371347%2C9151315480038319113%2C9151315480032964152&full\_bo...

Сервисы Начальная страница Почта Карты Маркет Новости Словари Видео Музыка Диск Mail.Ru Начальная страница Почта Образование Яндекс Почта Amazon.co.uk - Оп... Сервисы Яндекса Другие закладки

Отчеты Сообщения 8 594 Авторы 4 045 Задания

Все \* Избранное / \* Остальные Прочитанные / Непрочитанные С заметками С заданиями С ответами Пересечение Удаленные Скрытые 2

по дате публикации Экспорт Тексты Дубли Подсвечивать теги Только новые 1-50 из 4 932

Параметры по умолчанию

Ключевые слова  
вредоносное по

Период сегодня неделя месяц  
22 октября - 22 ноября 2020

время публикации  
время обнаружения

Объекты: выбрать  
 Взлом и кибератака  
 Вредоносное ПО  
 Кражи данных карт  
 Синий экран

Источники: все выбрать  
 Название платформы

посты  
 комментарии  
 репосты  
 изображения

Оценки: любые сбросить все  
 Позитивная  
 Позитивная (возможно)  
 Негативная  
 Негативная (возможно)

Народны Голас 7:31:47, 22 ноября

**Как мошенники пытались обмануть корреспондента «НГ» под видом сотрудников банка...**

Никогда не подумал бы, что я стану интересен для мошенников. Если они знают мои телефонные данные, соответственно, должны были знать и где я работаю. Оказалось, что я был не единственным, кому позвонили в этот день...

Было неожиданно, когда на один из мессенджеров от имени «Беларусбанка» (с изображением логотипа) мне позволили. Номер был из Российской Федерации (смотри на фото). Мошенник представился сотрудником службы безопасности и сообщил, что «банк вывел подозрительную операцию...

<http://www.yes.sk.by/2020/11/kak-moshenniki-pytalis-obmanut-korrespondenta-ng-pod-vidom-sotrudnikov-banka/>

Объект: Вредоносное ПО

Категории:

Теги:  
 Европа / Россия Европа / Беларусь / Минская область

Обнаружено 22 ноября 2020, 8:54:08

Пустельга Пустельгова 5:18:00, 22 ноября Репост

**❖ Гальдрастав целительской направленности "LE..."**

❖ Гальдрастав целительской направленности "LE GUÉRISSEUR NOIR"(ТЕМНЫЙ ЛЕКАРЬ)❖  
 #руны\_вереск\_ставы  
 #руны\_вереск\_ставы\_здоровье  
 Авторы: LAGERTHA и RAGNAR  
 Показать полностью...

Став создавался для лечения сложно излечимых заболеваний и долго не заживающих ран. Став полностью состоит из исландских рун, поэтому для тех, кто мало знаком с исландской магией и работой с гальдраставами, рекомендую перед началом работы почитать соответствующую литературу.  
 Став получился многопланового действия и на время ...

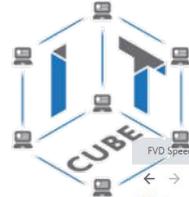
[https://vk.com/wall342524756\\_49901](https://vk.com/wall342524756_49901)

❖ РУНЫ и ВЕРЕСК ❖ 15:00:00, 22 ноября Пост

**❖ Гальдрастав целительской направленности "LE..."**

❖ Гальдрастав целительской направленности "LE GUÉRISSEUR NOIR"(ТЕМНЫЙ ЛЕКАРЬ)❖  
 #руны\_вереск\_ставы  
 #руны\_вереск\_ставы\_здоровье  
 Авторы: LAGERTHA и RAGNAR  
 Показать полностью...

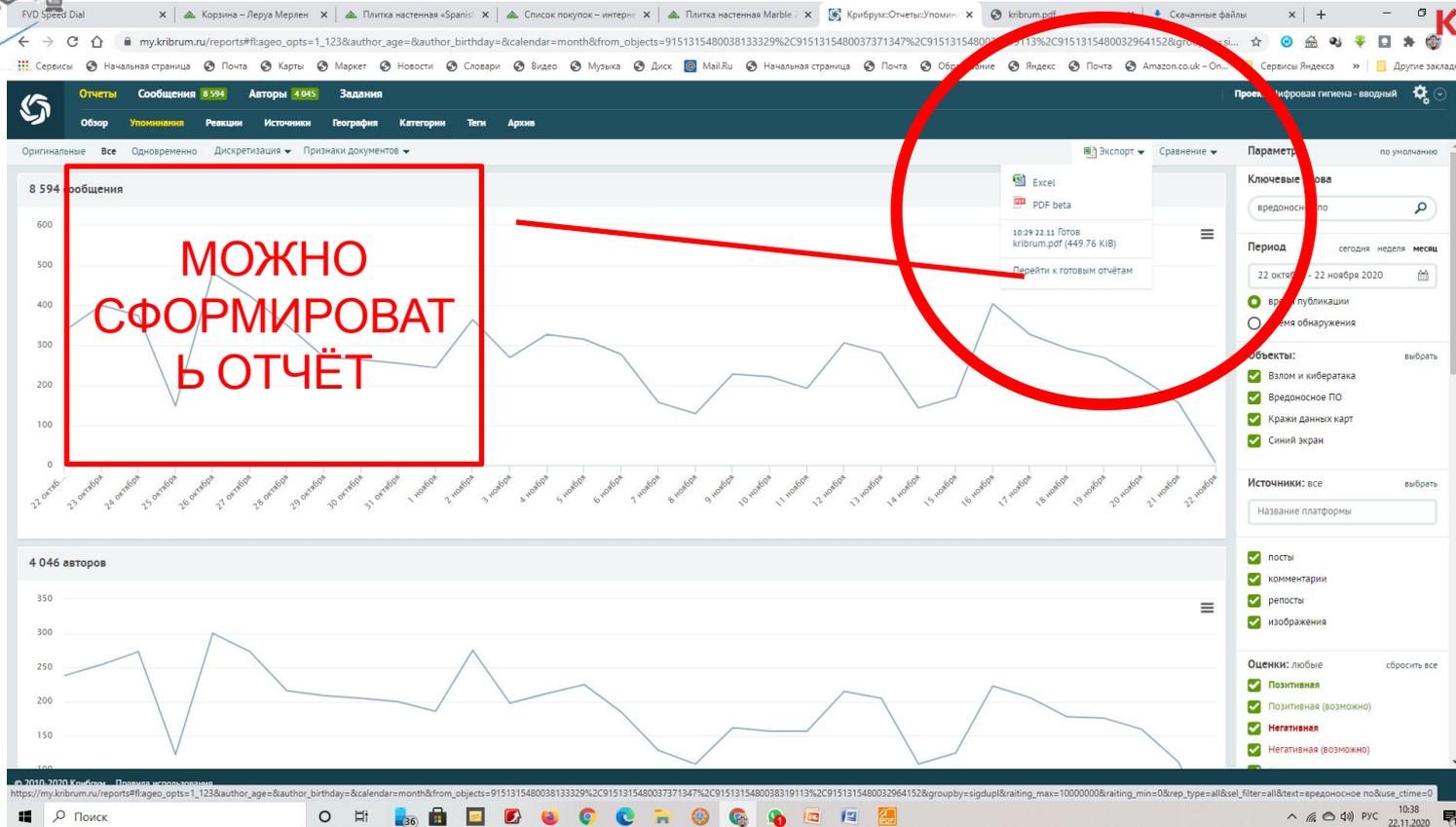
Став создавался для лечения сложно излечимых заболеваний и долго не заживающих ран. Став полностью состоит из исландских рун, поэтому для тех, кто мало знаком с исландской магией и работой с гальдраставами, рекомендую перед началом работы почитать соответствующую литературу.  
 Став получился многопланового действия и на время лечения ...



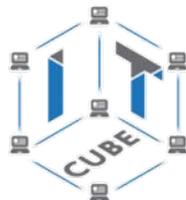
# ИЗУЧЕНИЕ ФЕЙКОВЫХ СООБЩЕНИЙ И ВРЕДОНОСНОГО ПО В СЕТИ ИНТЕРНЕТ



**КРИБРУМ**  
Мы слушаем сеть



# ИЗУЧЕНИЕ ФЕЙКОВЫХ СООБЩЕНИЙ И ВРЕДНОСНОГО ПО В СЕТИ ИНТЕРНЕТ



Начать kribrum.pdf x

Страницы

Цифровая гигиена - вводный

1

2

3

4

5

The image shows a PDF viewer interface for a document titled "Цифровая гигиена - вводный" (Digital Hygiene - Introductory). The document is displayed in a large window, and a sidebar on the left shows a table of contents with five pages. The first page is highlighted with a red box. The main content area shows the title, the КРИБРУМ logo, and the monitoring period: "Период мониторинга: 22.10.2020 00:00 - 22.11.2020 10:30".

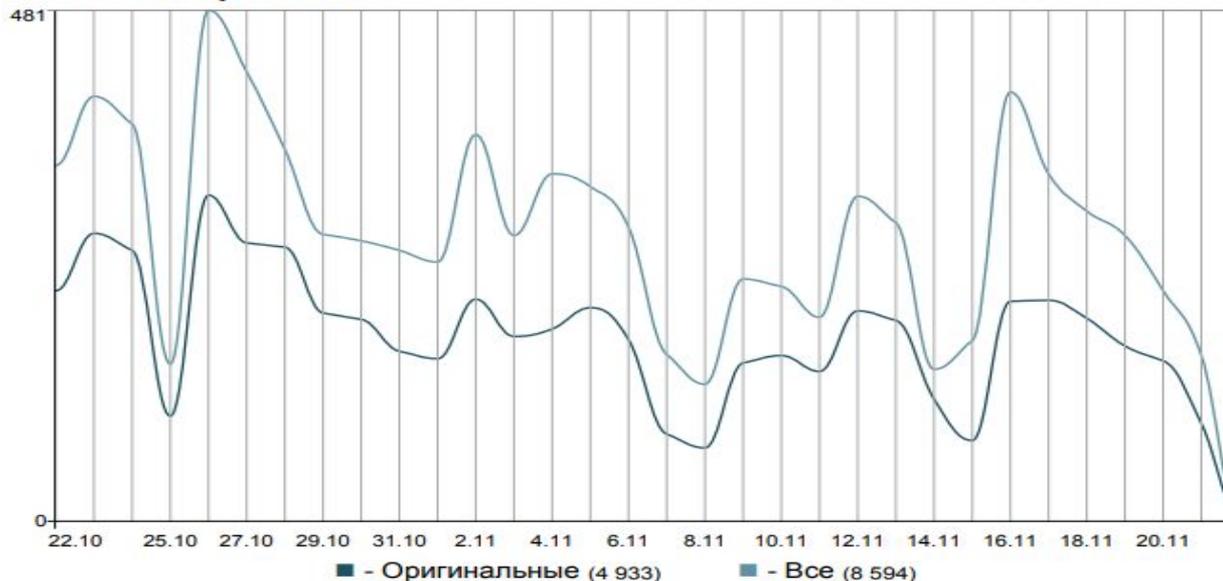


# ИЗУЧЕНИЕ ФЕЙКОВЫХ СООБЩЕНИЙ И ВРЕДНОСНОГО ПО В СЕТИ ИНТЕРНЕТ



1. Анализ временной динамики сообщений, какова сейчас ситуация в данной проблеме (Пик/ подъем/спад)

## Сообщения



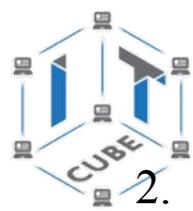
**КРИБРУМ**

Мы слушаем сеть [www.it-cube67.ru](http://www.it-cube67.ru)

<https://vk.com/itcube.smolensk>

[it-cube.smolensk@mail.ru](mailto:it-cube.smolensk@mail.ru)

<https://vk.com/club198370270>

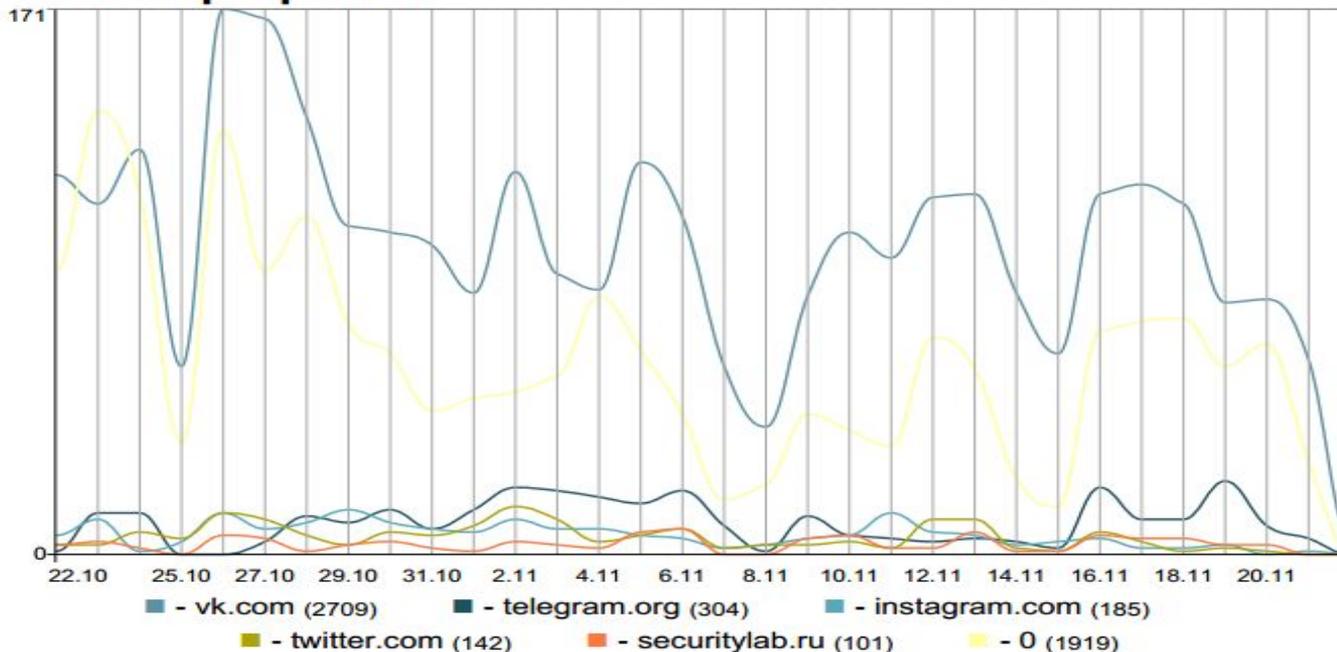


# ИЗУЧЕНИЕ ФЕЙКОВЫХ СООБЩЕНИЙ И ВРЕДНОСНОГО ПО В СЕТИ ИНТЕРНЕТ



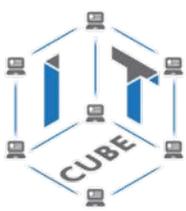
2. Популярные авторы, в каких источниках происходит наибольшее упоминание.

## Платформы



**КРИБРУМ**

Мы слушаем сеть



# ИЗУЧЕНИЕ ФЕЙКОВЫХ СООБЩЕНИЙ И ВРЕДНОСНОГО ПО В СЕТИ ИНТЕРНЕТ



## 3. Что посоветовать сделать при данной проблеме?

Группа сообщений 7 21 ноября 2020, 13:30:00 – 22 ноября 2020, 4:45:00 2 37 9 343 343

### Как почистить компьютер, чтобы не тормозил...

Как почистить компьютер, чтобы не тормозил

Периодически необходимо проводить чистку компьютера не только от пыли, но и от всевозможных временных файлов, пустых папок и бесполезных объектов. В противном случае он начнет показывать полностью... тормозить и упадет производительность.

Чтобы правильно провести чистку компьютера необходимо придерживаться определенного плана:

1. Удаление пыли из системного блока.
2. Проверка компьютера антивирусной программой на наличие **вредоносного ПО**.
3. Проведение ...

[https://vk.com/wall-108379670\\_16377](https://vk.com/wall-108379670_16377) 2 37 9 337 337

Объект: [Вредоносное ПО](#)

Категории:

Теги:

Топ источников: [vk.com](#) (7)

Обнаружено 21 ноября 2020, 16:17:46 – 22 ноября 2020, 10:17:02



**КРИБРУМ**

Мы слушаем сеть [www.it-cube67.ru](http://www.it-cube67.ru)

<https://vk.com/itcube.smolensk>

[it-cube.smolensk@mail.ru](mailto:it-cube.smolensk@mail.ru)

<https://vk.com/club198370270>

СОСТАВИТЬ И ПРЕДСТАВИТЬ ПЛАН  
ДЕЙСТВИЙ (ПОШАГОВОЙ ИНСТРУКЦИИ)  
ПО РЕШЕНИЮ ПРОБЛЕМЫ  
ЗАРАЖЕНИЯ ВИРУСАМИ КОМПЬЮТЕРА  
ИЛИ СМАРТФОНА.

Кейс 2. Занятие 2

Домашнее задание

Может быть  
сделано  
в  
любом удобном  
ВИДЕО





# СПАСИБО ЗА

Кибергигиена и работа с большими данными

[www.it-cube57.ru](http://www.it-cube57.ru)

<https://vk.com/itcube.smolensk>

[it-cube.smolensk@mail.ru](mailto:it-cube.smolensk@mail.ru)

# ВНИМАНИЕ