Аналитический отчет

# ИНФОРМАЦИОННАЯ ВОЙНА ПРОТИВ РОССИИ

## ЧАСТЬ 1. КОНСТРУИРОВАНИЕ ОБРАЗА ВРАГА

КРИБРУМ
Мы слушаем сеть

Подготовлено по заказу Центра политической информации

# Оглавление

# Предисловие

Сегодня является очевидным фактом, что Россия – объект крупномасштабного информационного воздействия, и в отношении нее развязана информационная война. **Цель развернутой кампании – дискредитация России на международной арене, конструирование в ее лице у населения зарубежных стран образа «врага».** Для достижения этой цели используются все возможные информационные каналы, все существующие классические и цифровые медиа.

**Представленный компанией «Крибрум» аналитический отчет «Конструирование образа врага» является первым в серии исследований методов и форм информационной войны.** Он еще раз подтверждает глобальный охват и высокую интенсивность информационного противостояния. На протяжении длительного времени на Россию навешивается ярлык «главной угрозы» суверенитету европейских стран, демократическим ценностям и западному образу жизни. В целях комплексного изучения информационной войны против России следующие исследования будут проводиться с использованием передовых возможностей как цифровой, так и традиционной социологии.

Если обратиться к истории, то в течение последних полутора столетий Россия находится под постоянным информационным воздействием, которое приостанавливалось всего несколько раз и на довольно непродолжительное время. За последние сто лет интенсивность информационных атак угасала дважды: в 40-е годы в период Второй мировой войны и в 90-е годы, когда страна по сути ушла с международной арены. Естественно, когда Россия вернулась, и российское руководство вновь стало отстаивать национальные интересы, механизмы информационной войны, успевшие слегка покрыться ржавчиной, снова были приведены в движение.

Сегодняшний виток дискредитационной компании в отношении России значительно отличается и от периода становления советского государства в 20-е и 30-е годы, и от эпохи «холодной войны». Если клише используются прежние («энергетическая зависимость», «шпионы» или «военная угроза»), то количество информационных каналов выросло многократно. За последние 20 лет колоссальным образом развились информационно-телекоммуникационные технологии, Интернет, появились глобальные социальные медиа, ставшие отдельным, самостоятельным «театром боевых действий». В этой связи размах идущей информационной войны носит беспрецедентный характер.

К сожалению, в результате информационного противоборства появились и первые жертвы: поколения людей, граждан стран Европы и Северной Америки,

с четко сконструированным ложным представлением о России, ее истории и уровне современного развития, о целях и устремлениях простых россиян.

В настоящее время все четче проявляется тотальный характер информационной войны против России. Помимо атак, связанных со значимыми событиями в России или с имеющими к ней прямое отношение (грузино-осетинский конфликт 2008 года, Олимпиада в Сочи, «Северный поток – 2», Чемпионат мира по футболу и др.), сегодня все отчетливей просматривается деятельность по перманентному поддержанию негативной повестки на достаточно высоком уровне. Это достигается путем периодических, ритмичных вбросов, компрометирующих Россию «фейк-ньюс», по сути – откровенной лжи.

Ценность и значимость представленного исследования компании «Крибрум» заключается в том, что на примере распространения «фейков» о России в социальной сети Twitter, с привязкой к определенным хэштегам, продемонстрированы размах информационной войны, спектр инструментов и механизмов конструирования в лице России и ее граждан образа «врага».

Тема восприятия России в мире многогранна и сложна, требует внимательного постоянного изучения с применением различных методов и подходов.

**Представленное исследование – первый шаг на пути к комплексному, научно-обоснованному осмыслению развернутой против России информационной войны.**

***Александр Гребенюк***

*доктор экономических наук,*

*заместитель директора по научной работе*

*ВШССН МГУ им. М.В. Ломоносова*

# Введение

В рамках настоящего исследования мы изучаем один из методов информационной войны – «конструирование образа врага». Под информационными войнами в данном отчете понимается **«целенаправленное широкомасштабное оперирование смыслами: создание, уничтожение, модификация, навязывание, блокирование носителей смыслов информационными методами для достижения поставленных целей»**[1].

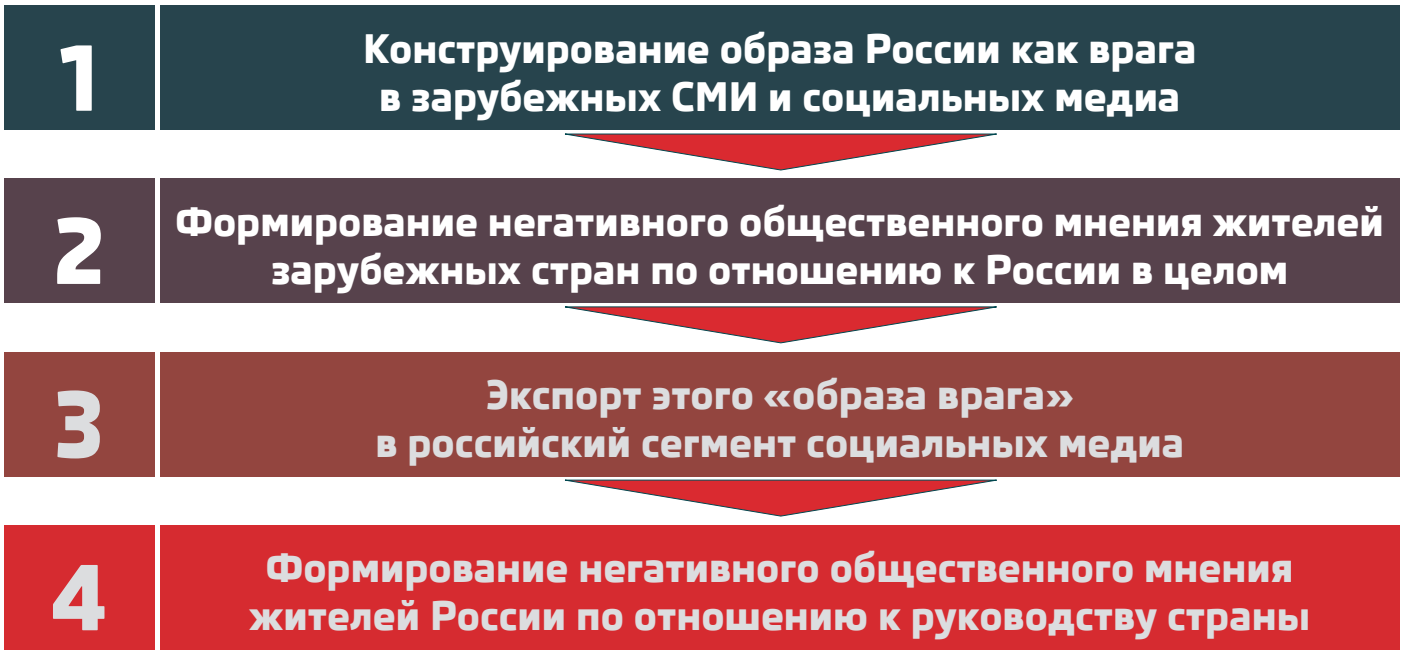
**Одним из наиболее эффективных методов на сегодняшний день является конструирование образа врага.** Образ врага оправдывает «военную риторику» одного государства и дискредитирует «страну врага» в глазах всего мира.

**Этот процесс содержит в себе многие формы оперирования смыслами:**

- **создание,**
- **модификацию,**
- **навязывание.**

Результаты настоящего исследования показывают, что **в странах Запада идет формирование негативного образа России, затем этот образ переносится в Россию и внедряется в сознание жителей России. Таким образом формируется негативное мнение российской аудитории относительно своей страны и ее руководства.**

**Этапы процесса экспорта «образа врага»:**




[1] С.П. Расторгуев. Введение в формальную теорию информационной войны. – М.: Вузовская книга, 2016, с. 3.

В настоящем исследовании были проанализированы русскоязычные социальные медиа и англоязычный информационный поток Twitter.

**Для первого исследования Twitter выбран потому, что это сервис с самой быстрой реакцией на актуальные общественно-политические события, который точно отражает состояние инфополя в целом.**

При первичном анализе были выделены хештеги, наиболее часто употребляемые Twitter-аккаунтами в сообщениях с обвинениями в адрес России. Затем был проанализирован информационный поток с 2014 года по май 2020 года по этим хештегам:

#StopRussianFascism
#RussianAgent
#RussianTerrorism
#WorldwakeupRussiainvadedUkraine
#Russianpoisoning
#ExpelRussiaFromUkraine
#RussiaAttacksUkraine
#stopRussia
#RussiainvadedUkraine
#RussianInterferenceAGAIN
#Russianpoison
#RussiaGate
#Russiantrolls
#Russianhackers
#RussianCollusion
#Russianbot
#RussiaHacking
#Russianassets
#RussianLies
#RepublicansForRussia
#republicanRuskies
#RussianSpy
#ReleaseTheRussiaReport
#stopRussianaggression
#RussianInterference
#blameRussia
#RussianPropaganda
#Russiaisanocupant
#terroRussia
#NoRussiaInPACE
#BanRussiaFromUNSC
#RussianBlackmail
#BanRussiafromSWIFT
#Russia2Trial

#PutinIsAMurderer
#PutinAtWar
#stopPutinism
#StopPutinsWarInUkraine
#PutinsLaundryBoy
#PutinsGOP
#PutinsHybridWar
#Putinsputridpuppet
#PutinsPuppets
#PutinsLittleBitches
#PutinBOTS
#RepublicansForPutin
#AllRoadsLeadToPutin
#StopPutin
#Putinterroristnumber1
#PutinTrumpVirus
#Putinsrevenge

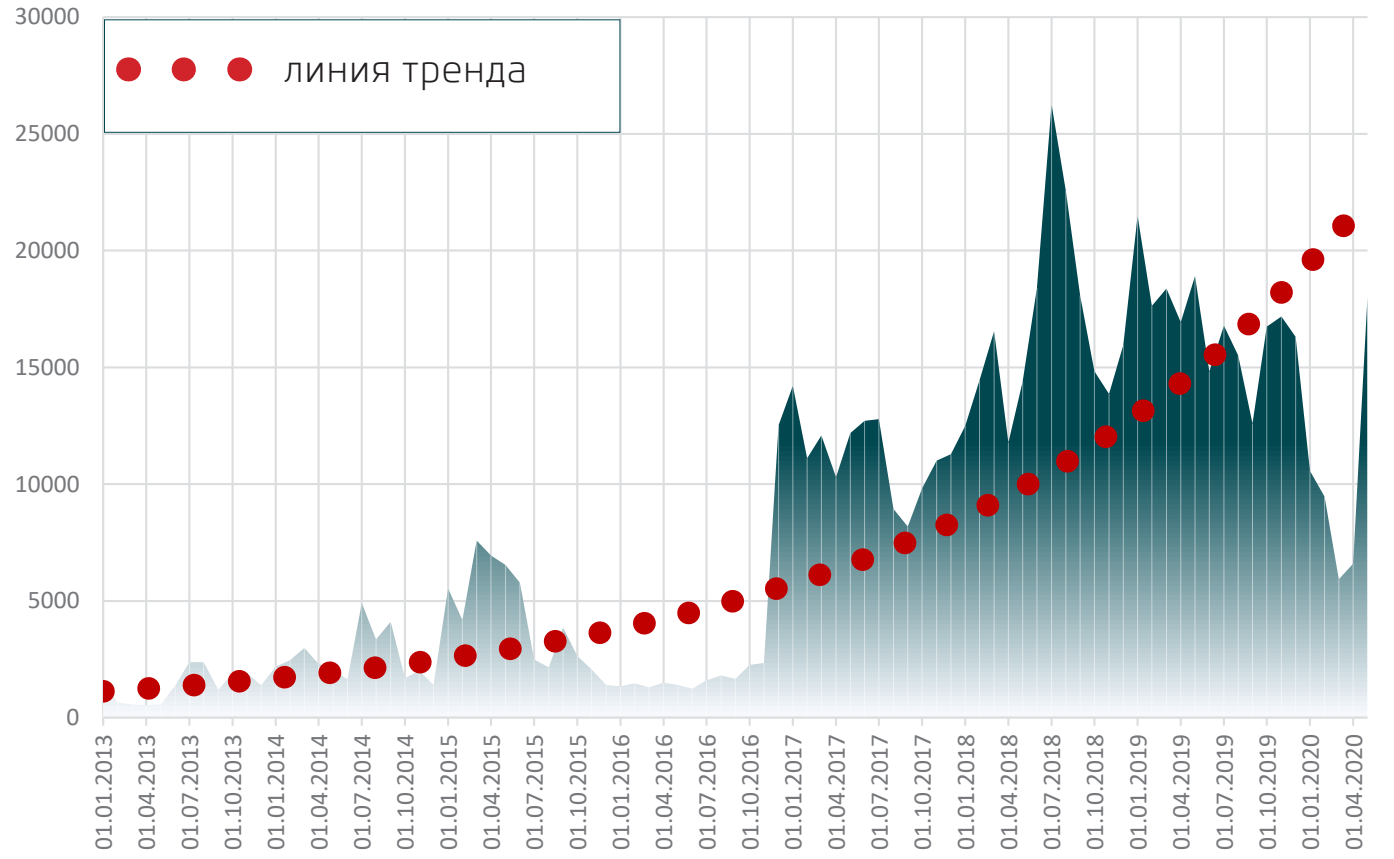
#Novichok
#NOcapitulationofUkraine
#GOPTraitors
#HybridWar
#RememberGenocideMay18
#MoscowMitch
#LeningradLindsey
#MoscowMitchHatesAmerica
#Skripal
#MagnitskyAct
#MoscowMules
#FreeUkrainianSailors
#stopputler
#RuskaKurwa
#MoscowMitchTraitor
#KyivAgainstMoscow
#CrimeanTatars
#CrimeaIsUkraine
#KGB

КРИБРУМ
Мы слушаем сеть

# Глава 1
# Общая информационная картина

Анализ распространения сообщений с обвинениями в адрес России показывает, что активно процесс конструирования образа врага начался со второй половины 2014 года после начала общественно-политических событий на Украине.

График 1. **Динамика сообщений в англоязычном сегменте**



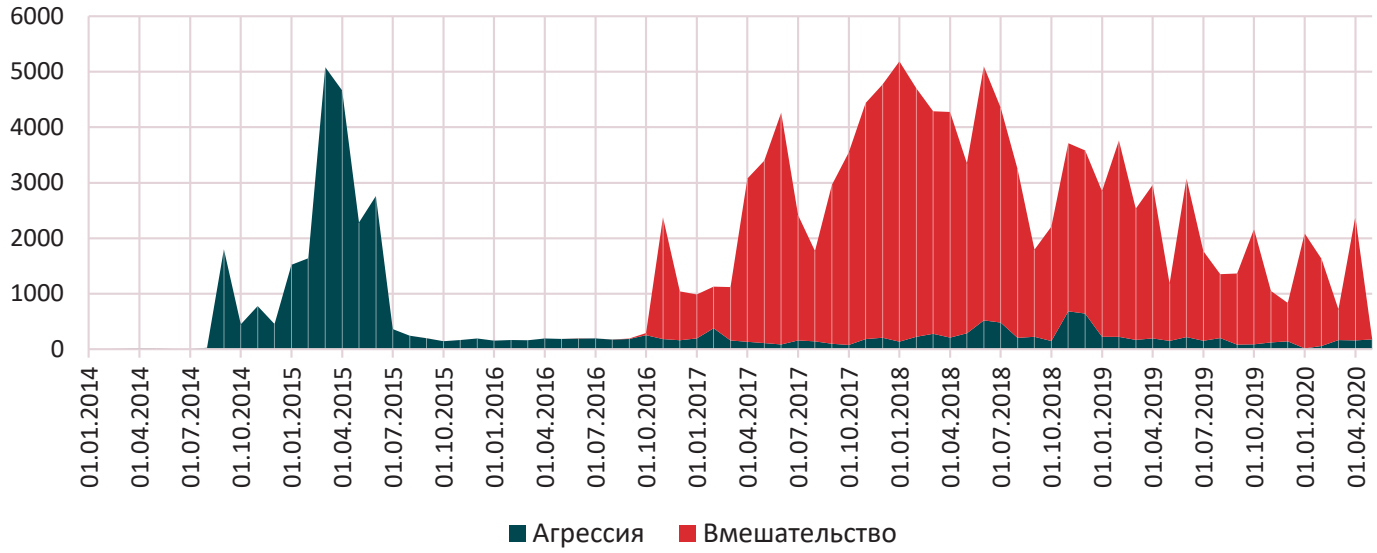

Изначально авторы привлекали аудиторию только в контексте событий на Украине, а основной стратегией были обвинения в агрессии.

В конце 2015 – 2016 году активность снижена в связи с электоральным циклом в США.

Резкий рост активности происходит в конце 2016 года. Это связано с окончанием выборного цикла и появлением нового тезиса о «российском вмешательстве».

Важно отметить, что произошла смена основной темы обвинений в адрес России. От **«агрессии»** перешли к **«вмешательству»** (График № 2 ).

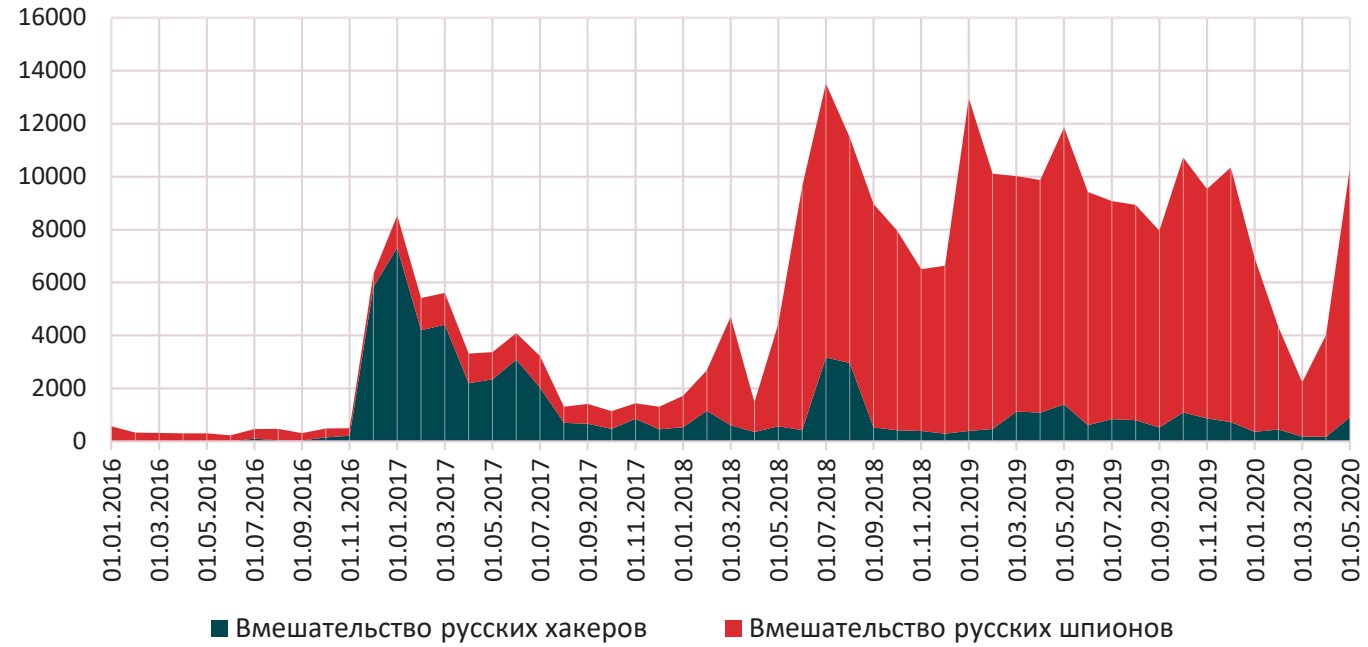
График 2. **Смена повестки в англоязычном сегменте**




В этот период растет количество сообщений с обвинениями России во вмешательстве во внутриполитические вопросы разных государств. Эти обвинения также неоднородны. Сначала во «вмешательстве» обвиняются «русские хакеры» и говорится об их возможной принадлежности к российским спецслужбам. Затем начинают писать о существовании специальных подразделений в ГРУ и ФСБ.

**Обвинения трансформировались от «русские хакеры, возможно связанные с российскими спецслужбами» на «российские спецслужбы»** (График № 3).

График 3. **Смена повестки в англоязычном сегменте**

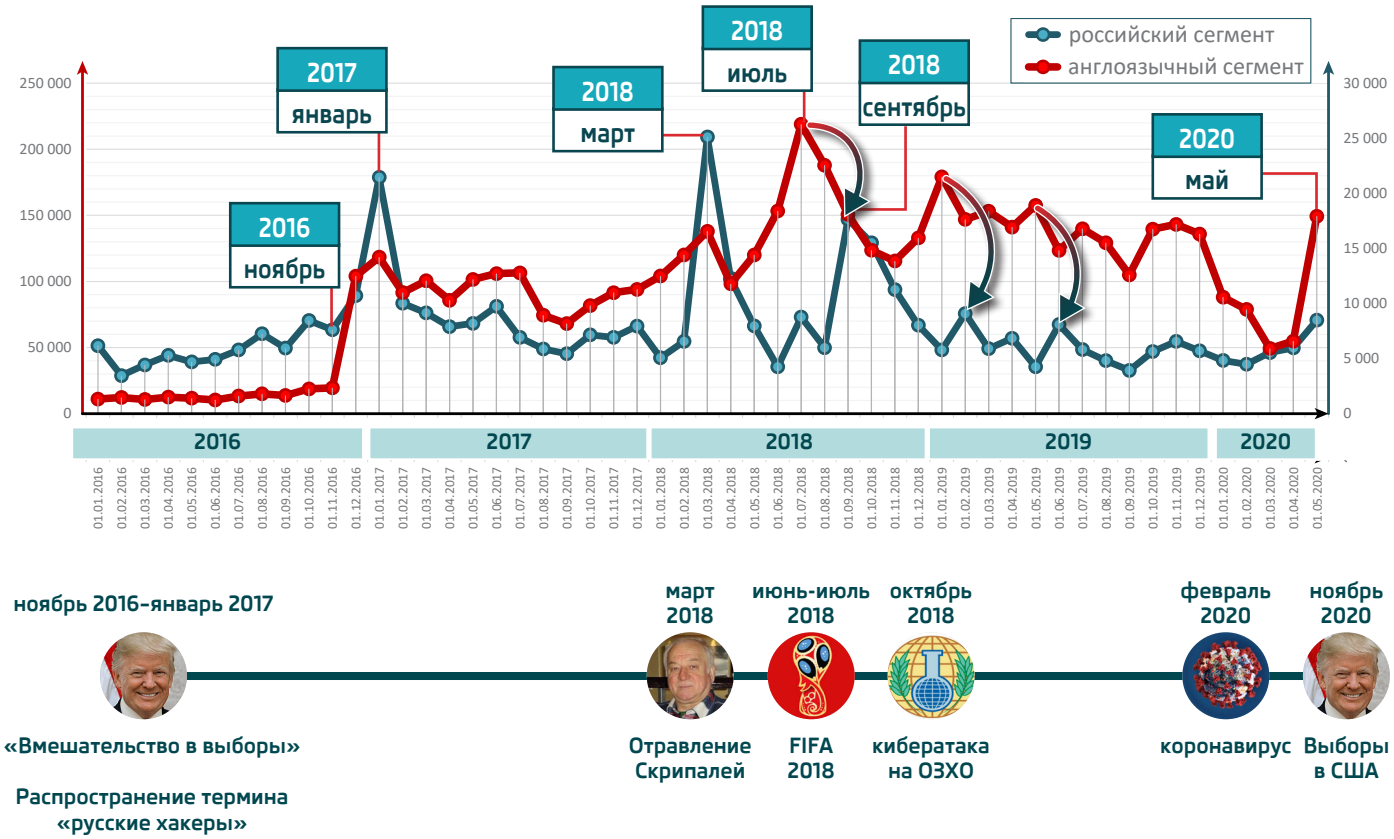


На графиках 3 и 4 наглядно видно, как **с 2014 по 2020 годы в англоязычном сегменте трансформировались обвинения в адрес России:**

## «Агрессия» – «Вмешательство русских хакеров» – «Вмешательство российских спецслужб» – Что дальше?

## Российские социальные медиа

График 4. **Хронология распространения сообщений о «русских хакерах» в российском и англоязычном сегментах социальных медиа**




Обвинения России во вмешательстве в выборы начали массово распространяться в иностранных СМИ и социальных медиа в ноябре-декабре 2016 года, перешли в русскоязычные социальные медиа в начале 2017 года. Основными распространителями информации являлись международные информационные агентства. Тезисы с бездоказательными обвинениями России во вмешательстве в дела иностранных государств постоянно присутствуют как в иностранной, так и российской информационной повестке вплоть до сегодняшнего дня.

В связи с распространением коронавирусной инфекции в мире, резко снижается число сообщений с обвинениями России в кибератаках, агрессивной внешней политике и по другим традиционным поводам.

Однако с приближением выборов президента США в ноябре 2020 года и деятельностью России по стабилизации отношений на внешнеполитической арене, активность иностранных и отечественных авторов вновь растет.

Поводами к обсуждению являются обвинения России в фальсификации статистики по коронавирусу, сообщения о взломе почты высших чиновников ФРГ российскими хакерами, публикации об атаках в Великобритании, Чехии, Польше и Грузии.

На графике 4 наглядно видны признаки **экспорта иностранной информационной повестки. На Западе формируется образ России относительно определенных событий, который затем переносится в российские социальные медиа. Этот образ всегда негативен!**

# Восприятие России в социальных медиа

Психологический и лингво-семантический анализ информационного пространства **иностранного сегмента** показывает, что у 35% пользователей Twitter образ России связывается с силовыми структурами РФ («ГРУ», «армия», «ФСБ», «спецслужба», «спецназ»); пользователи, не являющиеся медийными персонами, демонстрируют наличие признаков «киберфобии».

Пользователи реально опасаются киберугроз, **при этом не указывают на реальные факты или обстоятельства, создающие такую угрозу.**

Сейчас электоральный цикл в США находится в начальной стадии, и активная выборная деятельность еще не началась, однако уже сейчас американской аудиторией активно высказываются «прогностические» тезисы о неизбежном «вмешательстве русских хакеров» в предстоящие выборы.

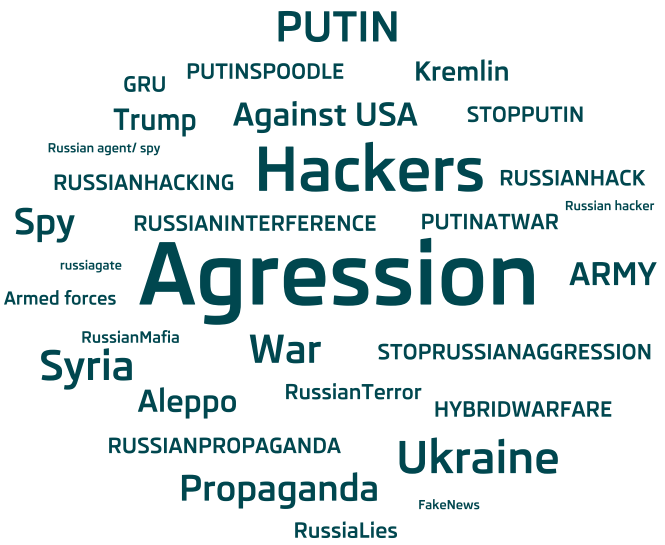
**В российском сегменте** социальных медиа образ «русские хакеры» активен, но, в отличие от иностранного сегмента, слабее связан с силовыми структурами РФ и проявлениями агрессии.

На формирование и поддержание подобных ассоциаций значительно повлияли многочисленные **бездоказательные обвинения России в кибератаках** на образовательные, медицинские учреждения и медиа разных стран, интенсивность которых резко возросла в 2019-2020 гг.

# **Облака тегов** (размер тегов соответствует количеству упоминаний)

## Зарубежный сегмент социальных медиа

### 2016




### 2018

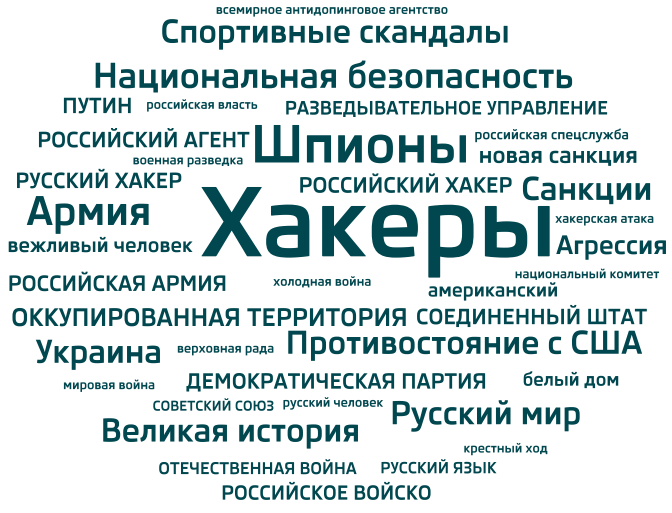

### 2020


## Российский сегмент социальных медиа

### 2016


### 2018


### 2020



Глава 2

# Использование хештегов

В распространении сообщений с обвинениями России активно используются устойчивые лингвистические конструкции и хештеги, позволяющие читателям быстро находить сообщения схожей тематики и направленности.

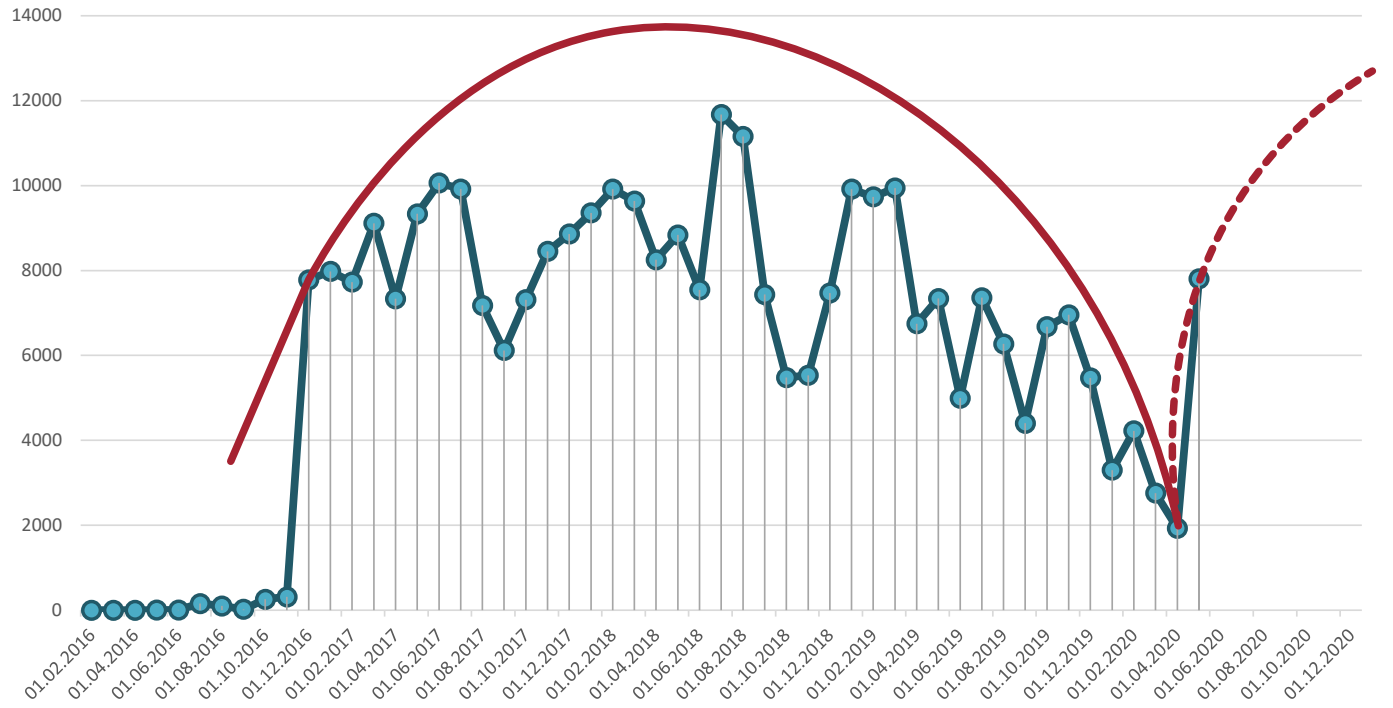
Большинство хештегов по содержанию универсальны и используются по любым поводам. Например, **#RussianTerrorism** и **#RussianLies** применяются в сообщениях с 2014 года. Использовались как во время острой фазы общественно-политических событий на Украине, так и в обвинениях в фальсификации статистики о коронавирусе.

**Обвинения России во вмешательстве в выборы иностранных государств являются одной из самых значительных тем за рубежом и в России.** В первую очередь, это касается темы выборов президента США в 2016 году. Задолго до подготовки и проведения избирательной кампании в социальных медиа распространялись обвинения в адрес «российских специалистов» в агитации за одного из кандидатов. Основной пик распространения этих публикаций пришелся на период с ноября 2016 года по январь 2017, когда начали массово распространять хештеги: **#putinsputridpuppet, #PutinsPuppets, #RussianHacking, #Russianhackers, #Russiantrolls** и т.д.

Эти теги остаются популярными до сих пор и используются для описания событий, уже не связанных с конкретными выборами в США.

**С мая 2020 года в преддверии новых выборов президента США в ноябре, их используют все чаще. Можно прогнозировать их рост в условиях очередной электоральной кампании.**

График № 6. **Динамика распространения сообщений о вмешательстве России во внутреннюю политику США** (англоязычный Twitter)




Россию также обвиняют по вопросам, не связанным с США.

Основными источниками создания и распространения хештегов с обвинениями в «оккупации» территории Крыма, части Донецкой и Луганской областей стали украинские пользователи.




Массово использовались хештеги: **#HybridWar, #StopPutinsWarInUkraine, #stoprussianaggression, #RussiaAttacksUkraine, #RussiainvadedUkraine**.

Теги публикуются в официальных заявлениях украинских политиков и в сообщениях пользователей вне зависимости от контекста и событий.

**Тема деятельности сотрудников российских спецслужб за пределами страны также является одной из основных в мировой информационной повестке.** Используются теги **#Russianpoison, #SalisburyAttack, #Novichok, #russianpoisoning, #Skripal, #RussianSpy, #RussianAgent, #GRU.**

График № 7. **Динамика распространения сообщений о «русских шпионах/агентах»** (англоязычный Twitter)

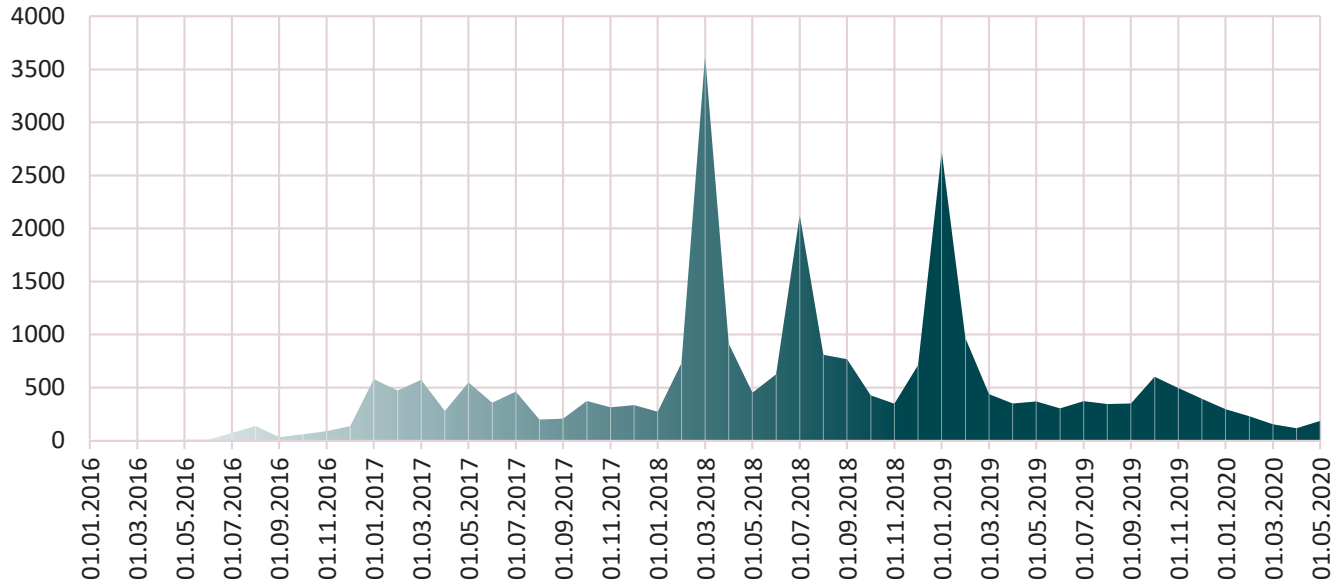
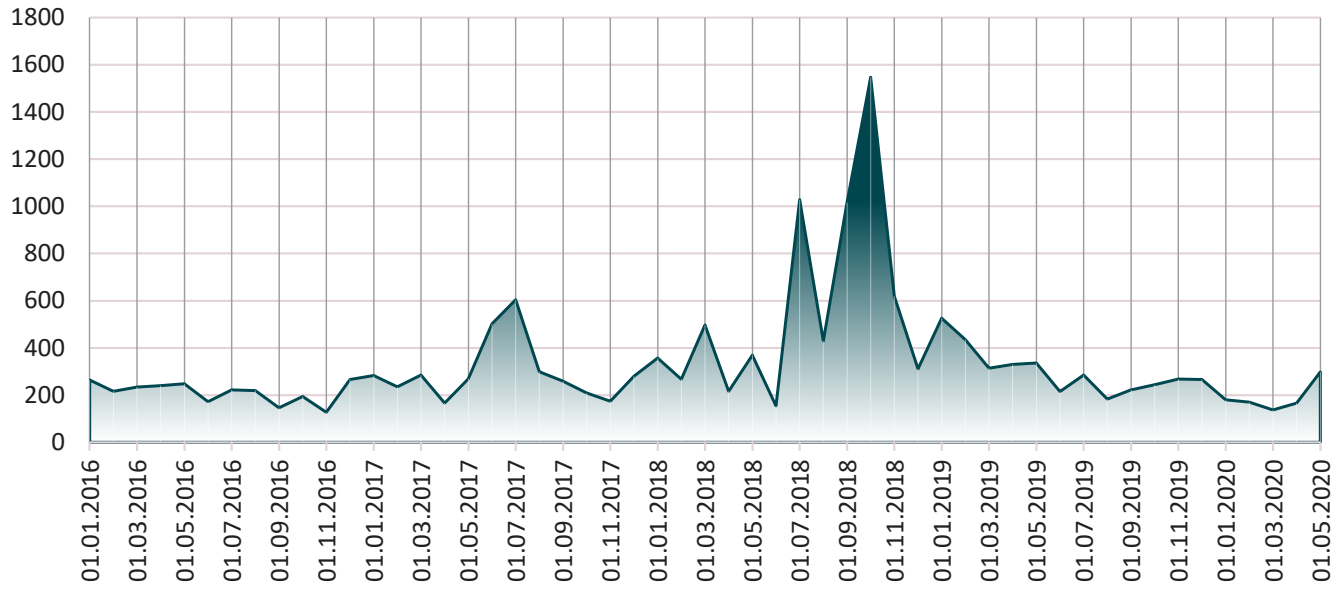



График № 8. **Динамика распространения сообщений о деятельности российских спецслужб** (англоязычный Twitter)




Изученные **хештеги используются в англоязычном сегменте Twitter более 6 лет и употребляются по различным поводам, часто вне зависимости от события или ситуации.** Например, использование хештега **stoprussianagression** по любой теме создает у читателя ощущение наличия «русской агрессии» повсюду, а 100 000 таких сообщений обеспечивают «достоверность» этой информации. **Использование хештегов упрощает создание, распространение и укрепление у интернет-аудитории тех самых смыслов, о которых говорится во введении.**

Глава 3

# Авторы сообщений

Авторами сообщений с обвинениями в адрес России являлись более 1,2 миллиона аккаунтов.

В западном сегменте **большое количество бездоказательных сообщений о русской агрессии распространяют популярные источники о спорте и музыке такие как Rolling Stone, BBC Sport и другие.** Эти источники расчитаны на массовую аудиторию и ее максимальный охват.

Информационная кампания достигает своей цели. Обычные люди, не являющиеся медийными персонами, пишут о несуществующей угрозе. **Возникает «киберфобия» – немотивированный страх перед кибератаками.**

## Зарубежный сегмент социальных медиа

### ТОП-10 ПОПУЛЯРНЫХ АВТОРОВ

| аккаунт/сообщество | подписчики | страна |
|---|---|---|
| Bill Maher | 11 075 971 | |
| BBC Sport | 8 423 205 | |
| Rolling Stone | 6 311 174 | |
| WikiLeaks | 5 511 067 | |
| Sky Sports Premier League | 4 796 779 | |
| Marco Rubio | 4 149 756 | |
| Economic Times | 3 588 564 | |
| CNN Politics | 3 479 338 | |
| The Hollywood Reporter | 3 230 295 | |
| George Takei | 2 993 885 | |

### ТОП-10 АКТИВНЫХ АВТОРОВ

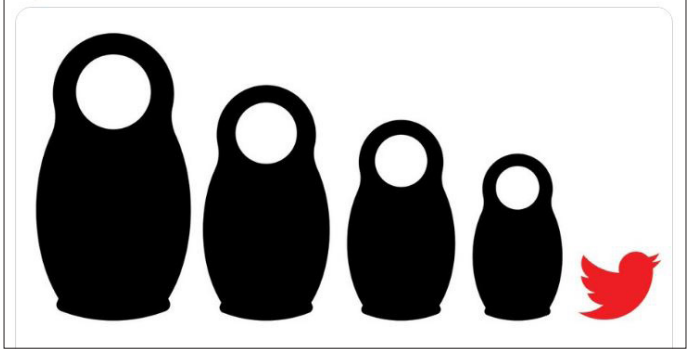
| аккаунт/сообщество | сообщения | страна |
|---|---|---|
| NeeVA | 9 028 | |
| Tunes4U2StayInside2 | 5 113 | |
| Puppet String News | 4 008 | |
| Relevantpµ‡epµ‡ë | 3 349 | |
| _tintin_ | 3 251 | |
| The Torn Curtain | 2 792 | |
| America's been Duped -- History and Civics | 2 411 | |
| Michael MacKay | 2 363 | |
| Libel Trump | 2 188 | |
| Peter W. Singer | 1 816 | |

# ПРИМЕРЫ ПУБЛИКАЦИЙ

**Rolling Stone**
@RollingStone

Here's what Russia's 2020 disinformation operations look like, according to two experts on social media and propaganda

Перевести твит



**George Takei**
@GeorgeTakei

Hackers, Hoaxes, & Hate, oh myyyy!

So excited to launch Season 2 of #OhMyyyPod! Our latest episode explores Russia's 2016 attack on our elections and features fascinating conversations with @TimothyDSnyder & @AndreaChalupa. Listen and subscribe today! po.st/RwcpsJ

**Marco Rubio**
@marcorubio

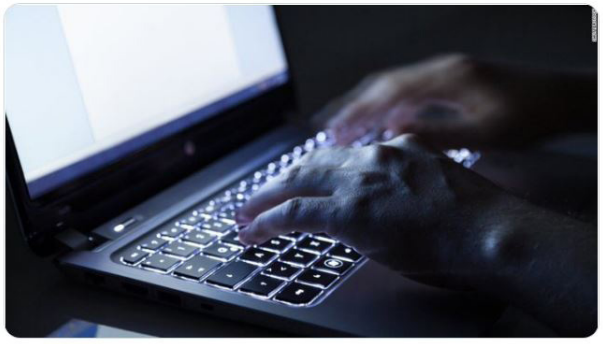
#Putin aligned agencies created a fake tweet from me warning of British spy threat to U.S. elections.

Then social media accounts aligned with #Russia & RT pushed the fake tweet.

And this is child's play compared to what they plan to do in the future.

**Economic Times** @EconomicTimes · 7 февр. 2018 г.
**Russian hackers** hunt hi-tech defense secrets


**CNN Politics** @CNNPolitics · 13 дек. 2016 г.
**Russian hackers** breached accounts of GOP individuals and groups before the election, US intel believes cnn.it/2gT366h



**Bill Maher** @billmaher · 21 окт. 2017 г.
If **Russia** is going to keep attacking America, then America really should fight back. #RussianTrollArmy #TrumpRussia #RussianPropaganda

# Российский сегмент социальных медиа

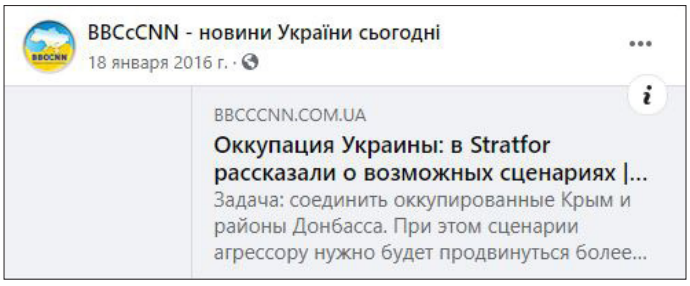
## ТОП-10 ПОПУЛЯРНЫХ АВТОРОВ

| аккаунт/сообщество | подписчики | страна |
|---|---|---|
| Повернись живим | 2 589 053 | |
| BBCcCNN - новини України сьогодні | 2 376 725 | |
| Пьяный Твиттер | 2 016 699 | |
| Умный Журнал | 1 803 390 | |
| Лепра | 1 603 795 | |
| Актуальна Мережа Новин | 1 594 666 | |
| Настоящее Время | 1 265 672 | |
| Meduza | 1 248 444 | |
| Mikheil Saakashvili | 1 234 367 | |
| bbcrussian | 1 091 943 | |

## ТОП-10 АКТИВНЫХ АВТОРОВ

| аккаунт/сообщество | сообщения | страна |
|---|---|---|
| Серёга Бойко | 2 213 | |
| Soft-Systems Servise | 1 891 | |
| ТСН.ua | 1 649 | |
| Сергей Лапиков | 1 380 | |
| Евгений Семененко | 784 | |
| Yakov Koltovskoy | 766 | |
| Олег Гончаров | 734 | |
| Георгий Субеда | 723 | |
| Сергей Мельников | 720 | |
| OWTA | 697 | |

**Наиболее популярными источниками распространения информации по формированию образа России как врага в российском сегменте социальных медиа являются украинские источники информации.**




Глава 4

# Примеры хронологии обвинений

Анализ информационной повестки в период, предшествующий обвинениям в адрес России в причастности к «хакерским атакам», выявлена следующая закономерность: **каждое такое «обвинение» предваряли геополитические события, способные стать началом улучшения отношений Российской Федерации и иного государства.**

Ниже приведены примеры хронологии использования фактов для дискредитации России в преддверии событий, способных оказать положительное влияние на отношения России с другими государствами. Поводом являются не сами факты, а информационная повестка в отношении России. **Задача псевдообвинений – воздействие на информационный фон.**

## Кибератаки на британские медицинские учреждения

### СООБЩЕНИЯ СМИ О КИБЕРАТАКЕ

**23.03.19 Издание «Forbes»**
Совершена кибератака на лондонскую компанию «Hammersmith Medicines Reseach»

**24.03.20 Отчет компании SecDev Group**
Количество атак на медучреждения во всем мире по сравнению с прошлым месяцем возросло на 47,5%

**14.04.20 Власти США и Великобритании**
Увеличивается количество кибератак против организаций, ведущих борьбу с коронавирусом

### ИНФОРМАЦИОННЫЙ ПОВОД ВЫГОДНЫЙ РОССИИ

**22.04.20 Постпред России в Генасамблее ООН**
Россия преложила проект резолюции о снятии санкций ради борьбы с коронавирусом

**22.04.20 Посол Великобритании в России Д. Бронер**
Спасибо МИД России и Аэрофлоту за помощь в возвращении граждан Великобритании на родину

**18.04.20 Пресс-секретарь Президента РФ Дмитрий Песков**
Предложенный Россией видеосаммит постоянных членов Совбеза ООН по обсуждению стратегии борьбы с COVID-19 может состояться в ближайшие дни

### ОБВИНИТЕЛЬНАЯ ИНФОРМАЦИОННАЯ КОМПАНИЯ

**03.05.20 Британский национальный центр кибербезопасности**
Университеты и исследовательские центры были атакованы киберпреступниками, которые действуют под патронатом правительства России, Китая и Ирана

**04.05.20 Спецслужбы Великобритании**
Российские хакеры пытаются украсть данные о вакцине COVID-19

**09.05.20 Британский национальный центр кибербезопасности**
Стоящая за атаками на британские лаборатории группа хакеров Базируется в Грузии и связана с Кремлем и российским службами безопасности

2020

## Кибератаки на медицинские учреждения Чехии

### СООБЩЕНИЯ СМИ О КИБЕРАТАКЕ

**11.12.19 Председатель больницы**
Больница города Бенешов подверглась кибератаке криптовирусом

**13.03.20 Издание «iDNES.cz»**
Больница чешского города Брно подверглась кибератаке

**27.03.20 Пресс-служба чешской полиции**
Осуществлена кибератака на психиатрическую больницу им. Космоносы в регионе Млада-Болеслав

### ИНФОРМАЦИОННЫЙ ПОВОД ВЫГОДНЫЙ РОССИИ

**09.04.20 Министерство обороны РФ**
Опубликовано письмо С. Шойгу с требованием вернуть России памятник маршала Конева

**12.04.20 Президент Чехии Милош Земан**
Демонтаж памятника – это глупая и смешная акция

### ОБВИНИТЕЛЬНАЯ ИНФОРМАЦИОННАЯ КОМПАНИЯ

**16.04.20 Комитет кибер- и информационной безопасности Чехии**
Предупреждение об угрозе новых кибератак

**18.04.20 Пресс-службы организаций**
Около 10 компаний сообщили о подозрительной активности на своих серверах

**20.04.20 Источник Lidovky**
IP-адреса ведут к России, однако анализ полученных данных еще не закончен

**21.04.20 Технический директор «ESET»**
Вредоносное ПО использованное для атаки на больницы в Чехии имеет российское происхождение

**21.04.20 Мнение редактора «Европейская правда»**
Признаки хакерских атак напоминают Эстонию в 2007 г., где накануне снесли «Бронзового солдата»

**21.04.20 Источник «Одесский курьер»**
Кибератаки на чешские больницы – месть МО РФ за снос памятника И.Коневу

2019 2020

## Кибератаки на образовательные учреждения Польши

### СООБЩЕНИЯ СМИ О КИБЕРАТАКЕ

**06.05.19** — **Центральное следственное бюро полиции Польши**

В школы Польши приходят электронные письма с информацией о минировании

**08.05.19** — **Центральная экзаменационная комиссия Польши**

О минировании сообщили 785 школ

### ИНФОРМАЦИОННЫЙ ПОВОД ВЫГОДНЫЙ РОССИИ

**09.04.20** — **Министр иностранных дел Польши Яцек Чапутович**

Важно улучшать отношения с Россией. Есть надежда, что странам удастся найти общий язык

**21.04.20** — **Министр иностранных дел России Сергей Лавров**

Ростки нормальных отношений между Москвой и Варшавой сохраняются

### ОБВИНИТЕЛЬНАЯ ИНФОРМАЦИОННАЯ КОМПАНИЯ

**11.05.20** — **Издание «RMF 24»**

За серией ложных сообщений о бомбах в школах в прошлом году стоит ГРУ Минобороны России

**12.05.20** — **Эксперт «TVPinfo» по российским спецслужбам Г. Кучинский**

Польша стала еще одним фронтом кибервойн, который возглавляет РФ

**11.05.20** — **Бывший глава Агентства внешней разведки Польши Г. Малецкий**

Кибератака выглядит как элемент гибридных действий России против Польши

**11.05.20** — **Бывший заместитель начальника Службы военной контрразведки Польши М. Матисяк**

Атака может включать элементы подрыва авторитета польского государства у молодежи

2019 — 2020

## Кибератаки на компанию Burisma

### СООБЩЕНИЯ СМИ О КИБЕРАТАКЕ

**15.11.19** — **Источник «Burisma». Официально не подтверждено**

Зафиксированы фишинг-атаки на сервера «Burisma» (по версии Area 1)

### ИНФОРМАЦИОННЫЙ ПОВОД ВЫГОДНЫЙ РОССИИ

**11.12.19** — **Президент США Дональд Трамп**

Улучшение отношений с Россией позволит расширить торговлю между странами

**16.11.19** — **Президент США Дональд Трамп**

Считаю своим долгом разобраться с коррупцией и действиями Джо Байдена, связанными с увольнением украинского прокурора, и с тем, что его сын получил миллионы долларов от украинской энергетической компании

### ОБВИНИТЕЛЬНАЯ ИНФОРМАЦИОННАЯ КОМПАНИЯ

**13.01.20** — **Отчет IT-компании «Area 1»**

Хакеры ГРУ получили данные учетных записей электронной почты сотрудников «Burisma» с целью похищения информации

**14.01.20** — **Редакция газеты «The Guardian»**

Утечка украденных данных может потенциально повлиять на процесс импичмента и выборы в США

**14.01.20** — **Глава «Area 1» О.Фальковиц для «The New York Times»**

Мы можем только предположить, что это повторение российского вмешательства в последние выборы

**14.01.20** — **Спикер палаты представителей США Нэнси Пелоси**

Тревожные сообщения о том, что российское правительство продолжает вмешиваться в наши выборы и подрывает нашу демократию, подчеркивают насущную необходимость действий

2019 — 2020

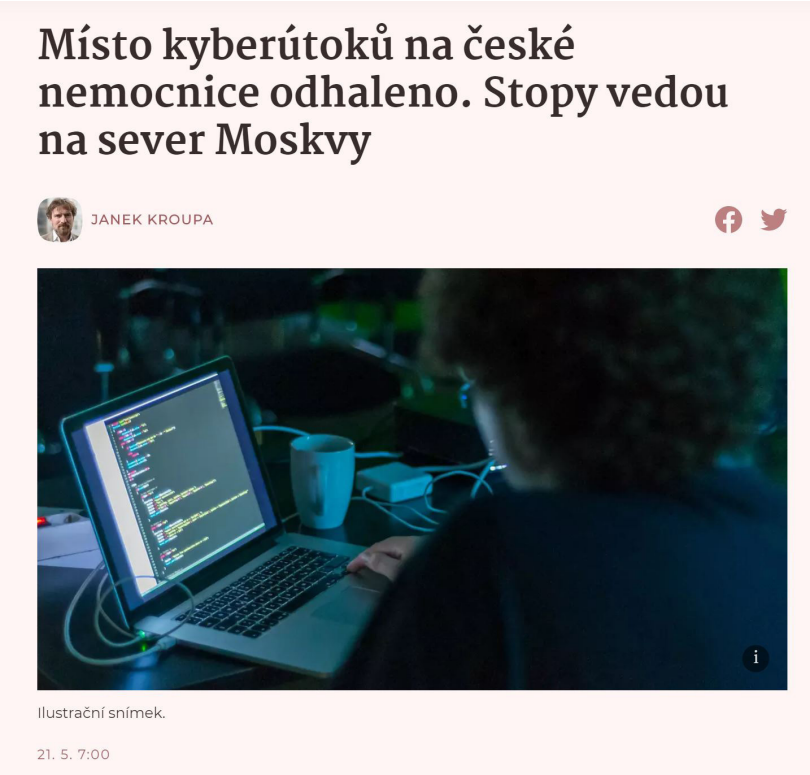
КРИБРУМ
Мы слушаем сеть

Глава 5

# Махинации с «доказательствами» участия русских хакеров

Доказательства, используемые авторами публикаций, зачастую не могут служить основанием для однозначных заявлений.

Так, после сообщений о кибератаках на лаборатории и медицинские учреждения в Чехии в марте 2020 года ряд СМИ и официальных лиц заявили о причастности к атакам граждан Российской Федерации. Подробности и обоснования обвинений были опубликованы в чешском издании Seznam Zprávy (Рисунок 1) с заголовком «Источник кибератак на чешские больницы раскрыт. Следы ведут на север Москвы». Согласно приведенному материалу, обвинения строятся лишь на одном факте аренды диапазона чешских IP-адресов, с которых проводились атаки, у компании Nexus ltd, офис которой зарегистрирован в Москве.


Místo kyberútoků na české nemocnice odhaleno. Stopy vedou na sever Moskvy

JANEK KROUPA

Ilustrační snímek.

21. 5. 7:00

Рисунок 1. **Скриншот публикации** (https://www.seznamzpravy.cz/clanek/misto-kyberutoku-na-ceske-nemocnice-odhaleno-stopy-vedou-na-sever-moskvy-106710)

Обвинения России кибератаках на грузинские медиа базируются в основном на одном заявлении посольства США в Грузии, без приведения каких-либо подробностей. Издание BBC ссылается на Британский национальный центр кибербезопасности, который отмечает, что «спецслужбы смогли с вероятностью более 95% определить, что именно ГРУ стояло за кибернападениями на Грузию в октябре 2019 года». Но в статье на сайте самого центра таких данных не обнаружено (Рисунок 2).


Рисунок 2. **Скриншот публикации** (https://www.ncsc.gov.uk/news/foreign-secretary-condemns-russia-s-gru-after-ncsc-assessment-of-georgian-cyber-attacks)

Согласно сообщениям польских СМИ (Рисунок 3), информация о бомбах и призыве их распространять появились на аккаунтах, «находящихся на серверах в Санкт-Петербурге и используемых ГРУ для распространения панических сообщений о ситуации в разных странах». В качестве доказательств приводится неофициальная информация от неких «польских следователей», однако самой этой информации нет. Каким образом нахождение серверов в Санкт-Петербурге связано с ГРУ, так же не объясняется.


Рисунок 3. **Скриншот публикации** (https://www.rmf24.pl/fakty/polska/news-news-rmf-fm-za-falszywymi-alarmami-bombowymi-w-trakcie-zeszl,nId,4487638)

**МНЕНИЕ ЭКСПЕРТА:**

*Во всех приведенных примерах в качестве доказательств используются данные, которые даже при поверхностном изучении вызывают больше вопросов, чем дают ответов.*

*Так, ip-адреса, зарегистрированные на российскую компанию или гражданина России, не дают оснований полагать, что за «атакой» стоят «русские хакеры», поскольку современные технологии позволяют скрывать и подменять ip-адреса, маршрутизируя трафик таким образом, чтобы оставить «следы» любой страны. Вместе с тем, довольно* ***сложно себе представить, что «специалисты», способные взломать довольно сложные механизмы защиты крупных компаний и государственных учреждений, не озаботились вопросами своей анонимности.***

*Зачастую в качестве доказательств участия «русских хакеров» рассматриваются фрагменты программного кода. Это довольно сомнительный аргумент, так как для взлома редко используется уникальный софт – это само по себе является демаскирующим признаком. Сегодня в открытом доступе можно найти довольно широкий инструментарий, поэтому даже если автор программы имеет «русские корни», это не значит, что им не воспользовался представитель другой страны.*

*Еще один распространенный пример – «модель проведения атаки» или «использование тех же методов, что и [а далее название любого инцидента информационной безопасности]. В этом случае тоже едва ли можно говорить о уникальности «того самого метода», поскольку он, как минимум, известен и тем, кто расследует инцидент, а зачастую и более широкому кругу лиц.*

*Также важно отметить, что все чаще официальными государственными лицами используются отсылки к докладам, расследованиям, комментариям сторонних частных компаний и экспертов. Вероятнее всего,* ***этот прием используется для снижения уровня ответственности за сделанное заявление и для устранения необходимости проводить проверку доказательной базы, которая попросту отсутствует.***

# Заключение

**Результаты исследования наглядно показывают ведение крупномасштабной информационной войны, имеющей четкий характер, этапы реализации и цель.**

**Эта информационная война направлена на формирование образа России, а также российских спецслужб и руководства страны, как мирового агрессора.**

**В качестве «оружия» используются обвинения в агрессии, вмешательстве во внутренние дела других стран, фальсификации информации, кибератаках. Однако доказательства, на которые ссылаются «эксперты», фактически отсутствуют.**

КРИБРУМ
Мы слушаем сеть

# ИНФОРМАЦИОННАЯ ВОЙНА ПРОТИВ РОССИИ

## ЧАСТЬ 1. КОНСТРУИРОВАНИЕ ОБРАЗА ВРАГА

Сегодня является очевидным фактом, Россия – объект крупномасштабного информационного воздействия, и в отношении нее развязана информационная война. Цель развернутой кампании – дискредитация России на международной арене, конструирование в ее лице у населения зарубежных стран образа «врага». Для достижения этой цели используются все возможные информационные каналы, все существующие классические и цифровые медиа.

121357, Москва,
ул. Верейская, 29, стр. 134
Тел: +7 499 372 5330
E-mail: info@kribrum.ru
Web: www.kribrum.ru

Москва 2020