

Аналитический отчет

2020

ИЮНЬ

ИНФОРМАЦИОННАЯ ВОЙНА ПРОТИВ РОССИИ

ЧАСТЬ 1. КОНСТРУИРОВАНИЕ ОБРАЗА ВРАГА



КРИБРУМ

Мы слушаем сеть

Подготовлено по заказу Центра политической информации

АНАЛИТИЧЕСКИЙ ОТЧЕТ

**ИНФОРМАЦИОННАЯ
ВОЙНА ПРОТИВ РОССИИ**

ЧАСТЬ 1.
КОНСТРУИРОВАНИЕ ОБРАЗА ВРАГА

Москва
2020

УДК 32.019.51

32.019.57

ББК 66.4

60.561.3

И74

И74 Лемэр Л. Г.

Информационная война против России. Часть 1. Конструирование образа врага» /
Л. Г. Лемэр, А. Н. Курицын, К. О. Семеновых, Э. Э. Меликов – Москва: Первое экономическое
издательство, 2020. – 28 с.

ISBN 978-5-91292-328-9

doi: 10.18334/9785912923289

Все права защищены. Никакая часть этой книги не может быть воспроизведена или использована в какой-либо форме, включая размещение в сети Интернет и в корпоративных сетях, а также запись в память ЭВМ для частного или публичного использования, без письменного разрешения владельца авторских прав.

Оглавление

Предисловие.....	6
Введение.....	8
ГЛАВА 1. Общая информационная картина.....	10
ГЛАВА 2. Использование хештегов.....	16
ГЛАВА 3. Авторы сообщений.....	19
ГЛАВА 4. Примеры хронологии обвинений.....	22
ГЛАВА 5. Махинации с «доказательствами» участия русских хакеров.....	25
Заключение.....	28

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 кампании 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 отчетливее 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 хештегам, 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.

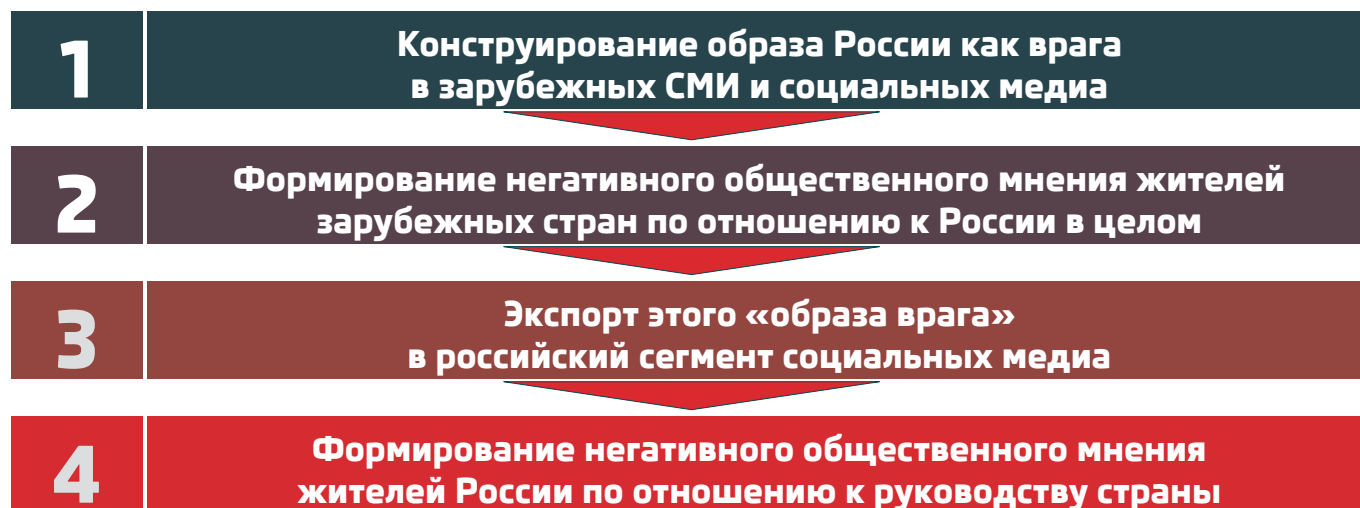
Одним из наиболее эффективных методов на сегодняшний день является **конструирование образа врага**. Образ врага оправдывает «военную риторику» одного государства и дискредитирует «страну врага» в глазах всего мира.

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 #Russian trolls #Russianhackers #RussianCollusion
 #Russianbot #RussiaHacking #Russianassets
 #RussianLies #RepublicansForRussia #republicanRuskies #RussianSpy
 #ReleaseTheRussiaReport #stopRussianaggression #RussianInterference
 #blameRussia #RussianPropaganda #Russiaisanoocupant
 #NoRussiaInPACE #BanRussiaFromUNSC #terroRussia
 #RussianBlackmail #BanRussiafromSWIFT
 #Russia2Trial

 #PutinIsAMurderer #Novichok
 #PutinAtWar #stopPutinism #NOcapitulationofUkraine
 #StopPutinsWarInUkraine #GOPTraitors #HybridWar
 #PutinsLaundryBoy #PutinsGOP #RememberGenocideMay18
 #PutinsHybridWar #Putinsputridpuppet #MoscowMitch #LeningradLindsey
 #PutinsPuppets #PutinsLittleBitches #MoscowMitchHatesAmerica #Skripal
 #PutinBOTS #RepublicansForPutin #MagnitskyAct #MoscowMules
 #AllRoadsLeadToPutin #StopPutin #FreeUkrainianSailors #stopputler
 #Putinterroristnumber1 #RuskaKurwa #MoscowMitchTraitor
 #PutinTrumpVirus #KyivAgainstMoscow
 #Putinsrevenge #CrimeanTatars
 #CrimealsUkraine
 #KGB

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



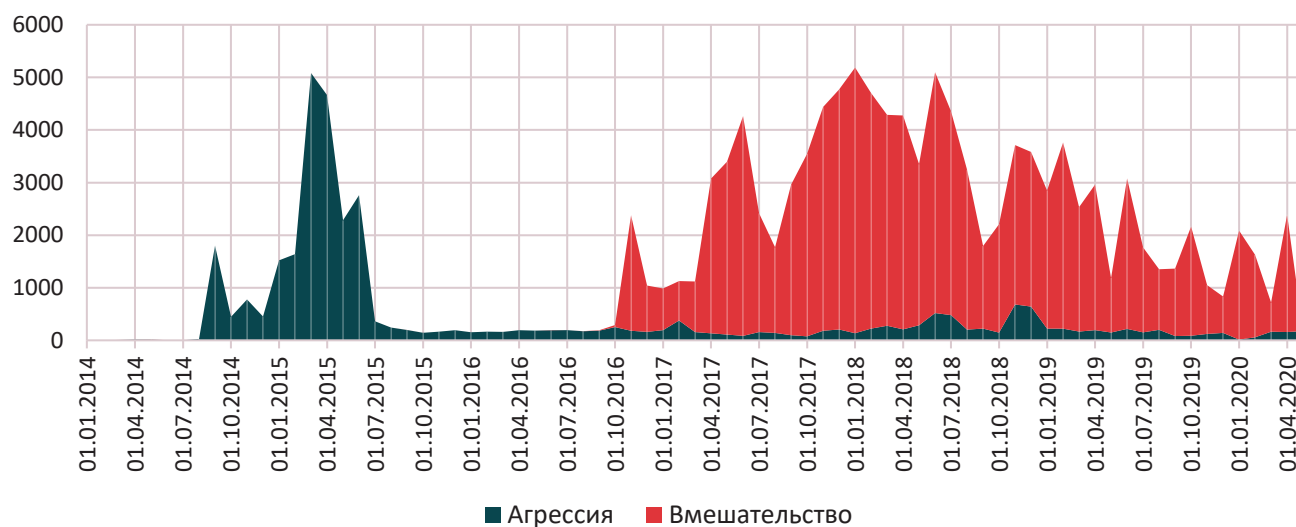
Изначально авторы привлекали аудиторию только в контексте событий на Украине, а основной стратегией были обвинения в агрессии.

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).

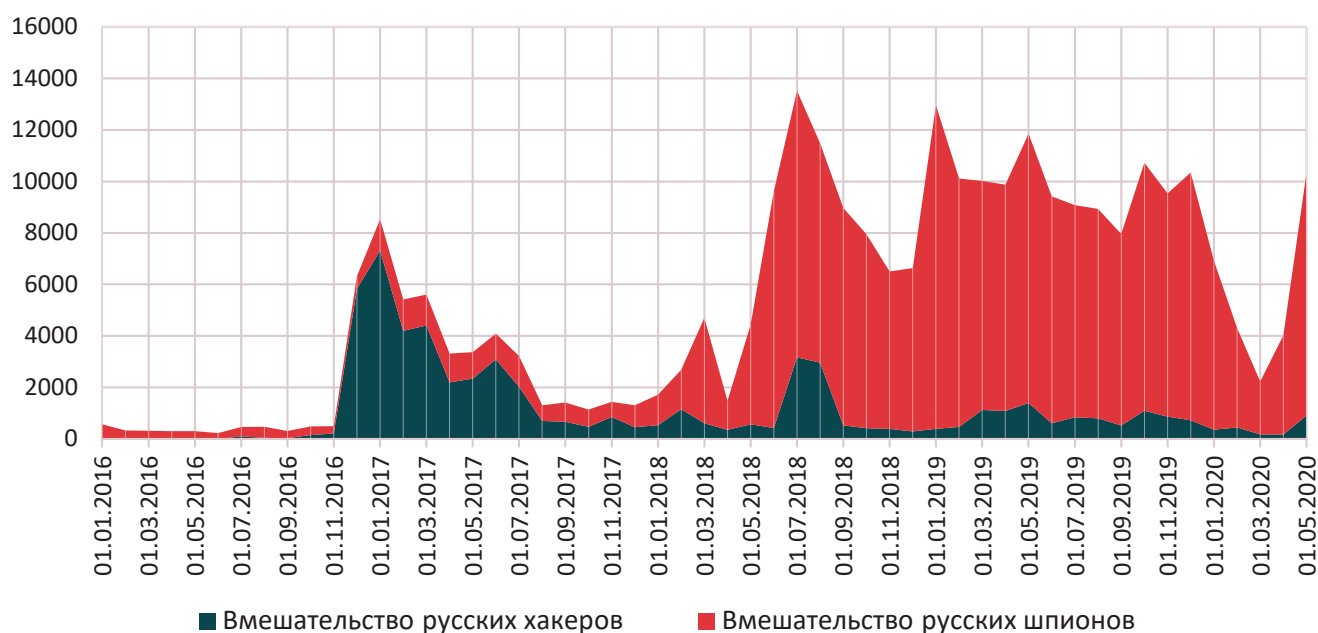
График 2. Смена повестки в англоязычном сегменте



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

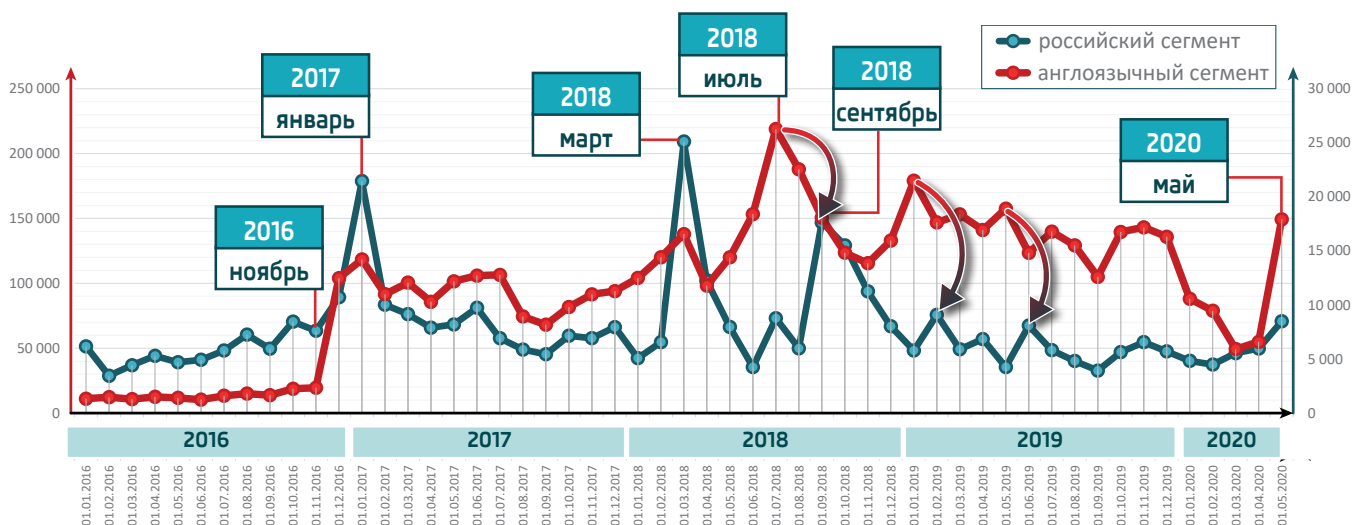


На графиках 2 и 3 наглядно видно, как с 2014 по 2020 год в англоязычном сегменте трансформировались обвинения в адрес России:

«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



ноябрь 2016–январь 2017



«Вмешательство в выборы»

Распространение термина «русские хакеры»



Отравление Скрипалей



FIFA 2018



кибератака на ОЗХО



коронавирус



Выборы в США

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

PUTIN
GRU PUTINSPOODLE Kremlin
Trump Against USA STOPPUTIN
RUSSIANHACKING Hackers RUSSIANHACK
RUSSIANINTERFERENCE PUTINATWAR Russian hacker
Spy Russiagate ARMED FORCES
Aggression ARMY
Syria RussianMafia War STOPRUSSIANAGGRESSION
Aleppo RussianTerror HYBRIDWARFARE
RUSSIANPROPAGANDA Ukraine
Propaganda FakeNews
Russiailies

2018

WalkAway ImpeachTrump
WAR
ARMY Agression investigation
PUTINSPOODLE Weapon terrorist
MUELLER Putin RUSSIANHACKING
Kremlin GRU RUSSIAGATE
RussianSpy SPYGATE RussianCollusion CRIMEA
TRUMP RUSSIA TRUMP Ukraine
Obama Agains USA OBAMAGATE DONBASS
Russian Interference
PUTINATWAR Resist
ELECTION

2020

FakeNewsMedia RussianPropaganda
Propaganda MEDIA LEAK
FakeNews
RUSSIAN TROLL CORRUPT DEEPSTATECORRUPTION
GRU RUSSIAN HACKER Hacker
RUSSIAGATE RussianAgent
Against USA SPYGATE investigation
Obama CAMPAIGN justice
RUSSIANCOLLUSION SPYGATE
OBAMAGATE ELECTION RussianInterference
HELL PUTINATWAR EVIDENCE scandal
WALKAWAY Agression RUSSIANHOAX
Ukraine PUTINKILLSCHILDREN TRUTH
PRESIDENT Putin

Российский сегмент социальных медиа

2016

ВОЕННАЯ РАЗВЕДКА
РАЗВЕДЫВАТЕЛЬНОЕ УПРАВЛЕНИЕ
специальное назначение морская пехота
генеральный штаб
национальная безопасность
РОССИЙСКАЯ СПЕЦСЛУЖБА
Агенты
РОССИЙСКИЙ АГЕНТ
российская армия
Безопасность
РОССИЙСКИЙ ХАКЕР
российский шпион
русская армия
Хакеры новая санкция
РОССИЙСКИЙ СОЮЗ
русский мир
гражданская война
РУССКИЙ ХАКЕР
хакинг
хакерская атака
ВЕЛИКАЯ ИСТОРИЯ
ОТЕЧЕСТВЕННАЯ ВОЙНА
БОЕВОЕ ДЕЙСТВИЕ Агрессия
русийская армия
диверсионная группа
вооруженный конфликт
ОККУПИРОВАННАЯ ТЕРРИТОРИЯ
русский мир
крестный ход
российская агрессия
предвыборная кампания
Выборы

2018

Великая история
засекреченная структура
ОТЕЧЕСТВЕННАЯ ВОЙНА
РОССИЙСКАЯ СПЕЦСЛУЖБА Украина
элитный боец
специальное назначение
Агенты
РОССИЙСКИЙ ШПИОН
российская разведка
разведывательное управление
БЫВШИЙ ПОЛКОВНИК
РОССИЙСКИЙ ХАКЕР
соединенный штат
большой дом
Армия Хакеры США
вооруженная сила
британский мид
РУССКИЙ ХАКЕР
Противостояние с Великобританией
РОССИЙСКИЙ ДИПЛОМАТ
британская спецслужба
БРИТАНСКАЯ ВЛАСТЬ
Дипломатия
РОССИЙСКИЙ МИД
БРИТАНСКИЙ СОЛСБЕРИ
нервно-паралитический газ
ОТРАВЛЯЮЩЕЕ ВЕЩЕСТВО
Химическое оружие
новая санкция
северный поток
Санкции

2020

всемирное антидопинговое агентство
Спортивные скандалы
Национальная безопасность
ПУТИН
российская власть
РАЗВЕДЫВАТЕЛЬНОЕ УПРАВЛЕНИЕ
российская спецслужба
РОССИЙСКИЙ АГЕНТ ШПИОНЫ
военная разведка
новая санкция
РУССКИЙ ХАКЕР
РОССИЙСКИЙ ХАКЕР Санкции
Армия Хакеры Агрессия
вежливый человек
РОССИЙСКАЯ АРМИЯ
холодная война
национальный комитет
американский
ОККУПИРОВАННАЯ ТЕРРИТОРИЯ СОЕДИНЕННЫЙ ШТАТ
Украина
верховная рада
Противостояние с США
мировая война
ДЕМОКРАТИЧЕСКАЯ ПАРТИЯ
белый дом
СОВЕТСКИЙ СОЮЗ
русский человек
Русский мир
крестный ход
ОТЕЧЕСТВЕННАЯ ВОЙНА
РУССКИЙ ЯЗЫК
РОССИЙСКОЕ ВОЙСКО

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.

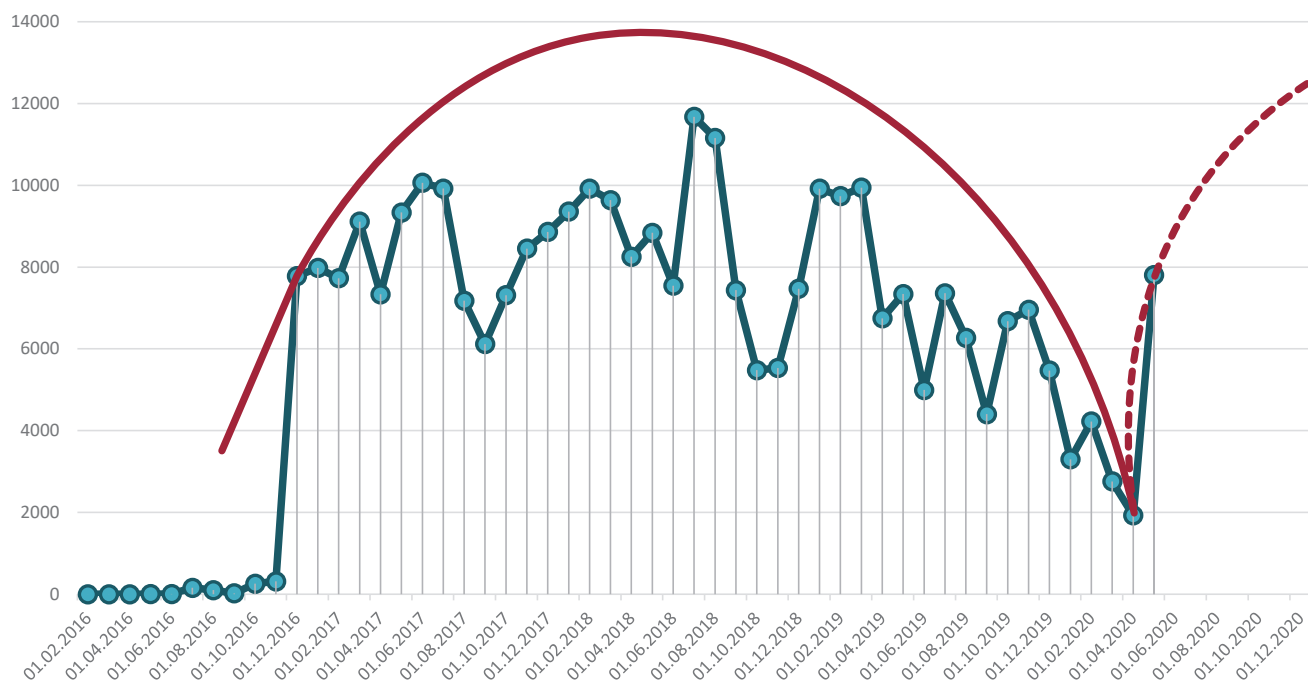
Большинство хештегов по содержанию универсальны и используются по любым поводам. Например, **#RussianTerrorism** и **#RussianLies** применяются в сообщениях с 2014 года. Использовались как во время острой фазы общественно-политических событий на Украине, так и в обвинениях в фальсификации статистики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

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

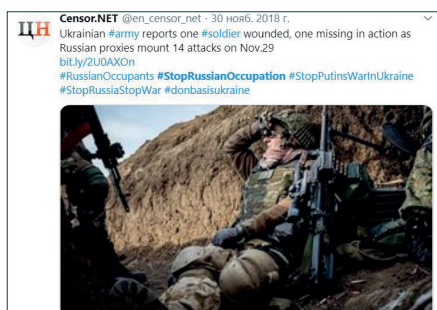
С мая 2020 года в преддверии новых выборов президента США в ноябре их используют все чаще. Можно прогнозировать их рост в условиях очередной электоральной кампании.

График № 5. 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 № 6. Динамика распространения сообщений о «русских шпионах/ агентах» (англоязычный Twitter)

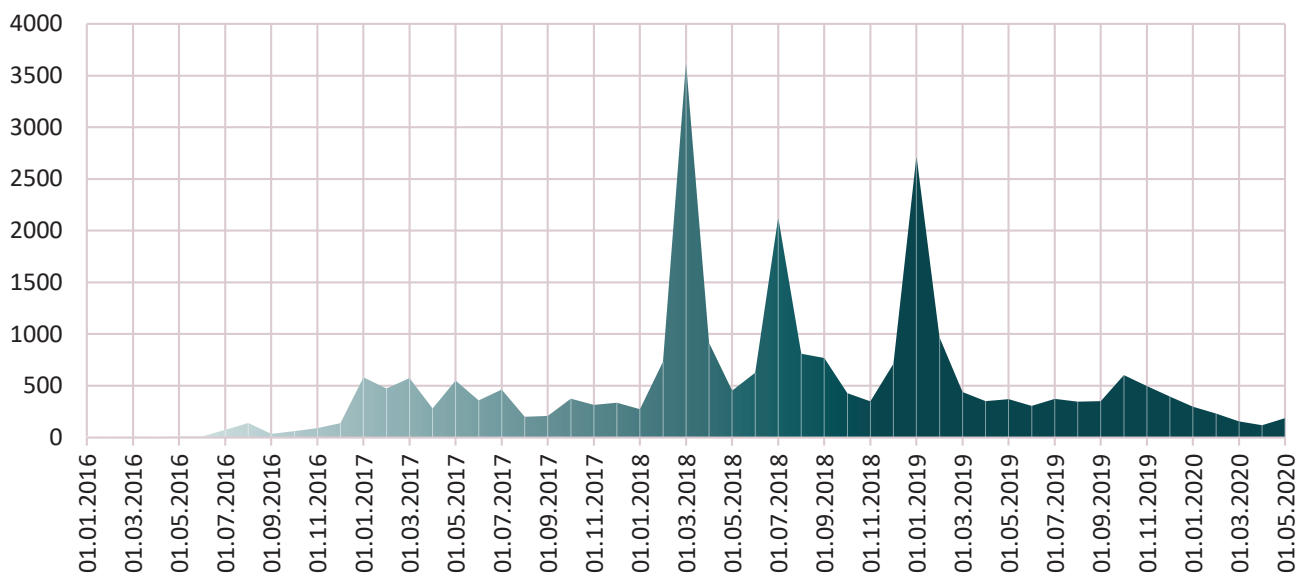
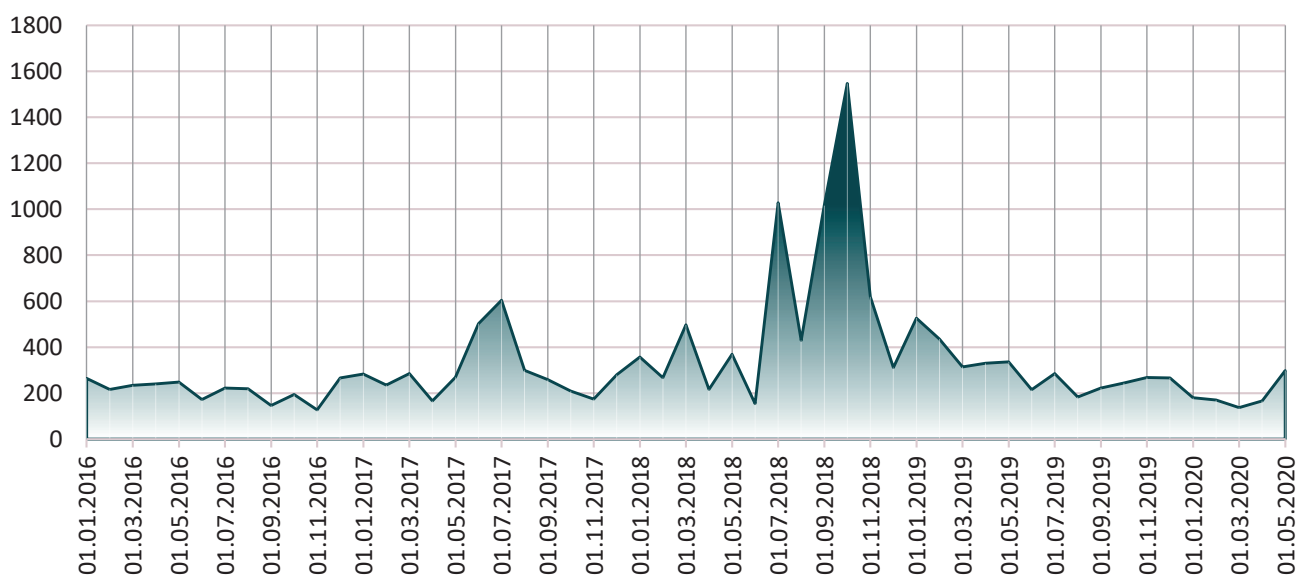


График № 7. Динамика распространения сообщений о деятельности российских спецслужб (англоязычный Twitter)











































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 **stoprussianaggression** 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 рассчитаны 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			ТОП-10 АКТИВНЫХ АВТОРОВ		
аккаунт/сообщество	подписчики	страна	аккаунт/сообщество	сообщения	страна
 Bill Maher	11 075 971		 NeeVA	9 028	
 BBC Sport	8 423 205		 Tunes4U2StayInside2	5 113	
 Rolling Stone	6 311 174		 Puppet String News	4 008	
 WikiLeaks	5 511 067		 Relevantрусские	3 349	
 Sky Sports Premier League	4 796 779		 _tintin_	3 251	
 Marco Rubio	4 149 756		 The Torn Curtain	2 792	
 Economic Times	3 588 564		 America's been Duped -- History and Civics	2 411	
 CNN Politics	3 479 338		 Michael MacKay	2 363	
 The Hollywood Reporter	3 230 295		 Libel Trump	2 188	
 George Takei	2 993 885		 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

Economic Times @EconomicTimes · 7 февр. 2018 г.

Russian hackers hunt hi-tech defense secrets

857 просмотров 0:20 / 3:15

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

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

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.

Bill Maher @billmaher · 21 окт. 2017 г.

If **Russia is going to keep attacking America**, then America really should fight back. #RussianTrollArmy #TrumpRussia #RussianPropaganda

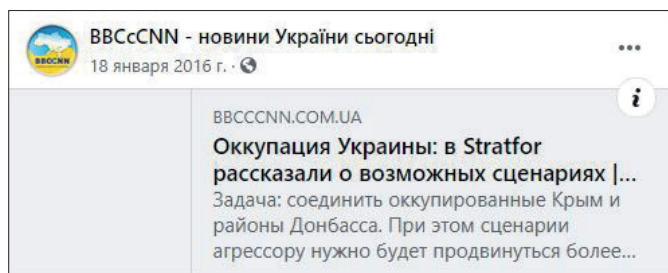
Посетить youtube.com

280,2 тыс. просмотров RED DON 0:02 / 4:27

Российский сегмент социальных медиа					
ТОП-10 ПОПУЛЯРНЫХ АВТОРОВ			ТОП-10 АКТИВНЫХ АВТОРОВ		
аккаунт/сообщество	подписчики	страна	аккаунт/сообщество	сообщения	страна
 Повернись живим	2 589 053		 Серёга Бойко	2 213	
 ВВСсCNN - новини України сьогодні	2 376 725		 Soft-Systems Servise	1 891	
 Пьяный Твиттер	2 016 699		 TCH.ua	1 649	
 Умный Журнал	1 803 390		 Сергей Лапиков	1 380	
 Лепра	1 603 795		 Евгений Семенов	784	
 Актуальна Мережа Новин	1 594 666		 Yakov Koltovskoy	766	
 Настоящее Время	1 265 672		 Олег Гончаров	734	
 Meduza	1 248 444		 Георгий Субеда	723	
 Mikheil Saakashvili	1 234 367		 Сергей Мельников	720	
 BBC NEWS	1 091 943		 OWTA	697	

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

Примеры публикаций



ВВСсCNN - новини України сьогодні
18 января 2016 г.

ВВССNN.COM.UA
Оккупация Украины: в Stratfor рассказали о возможных сценариях [...]
Задача: соединить оккупированные Крым и районы Донбасса. При этом сценарии агрессору нужно будет продвинуться более...



Mikheil Saakashvili
5 апреля 2014 г.

Война приближается
Почему сумасшедший царь России не успокоится
Михеил Саакашвили - 4 апреля 2014 - Статья в Foreign Policy
В начале марта, после инсценировки референдума в Крыму под дулами автоматов Калашникова, Россия приступила к процессу аннексии региона и заложила фундамент, по словам Москвы, для «новых политико-правовых реалий», так сказать, новая русская парадигма для беззаконного мира. Как сказала канцлер Германии Ангела Меркель в своем выступлении в Бундестаге 13 марта, Россия принесла закон джунглей в цивилизованный мир. Для тех из нас, кто пережил попытки Владимира Путина предотвратить последствия того, что он называет «величайшей геополитической катастрофой» 20-го века - распад Советского Союза - то, что происходит в Украине не является неожиданным. Но это и не последний акт спектакля.

Глава 4

Примеры хронологии обвинений

Анализ информационной повестки в период, предшествующий обвинениям в адрес России в причастности к «хакерским атакам», выявил следующую 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 образовательные учреждения Польши



Кибератаки на компанию Burisma



Глава 5

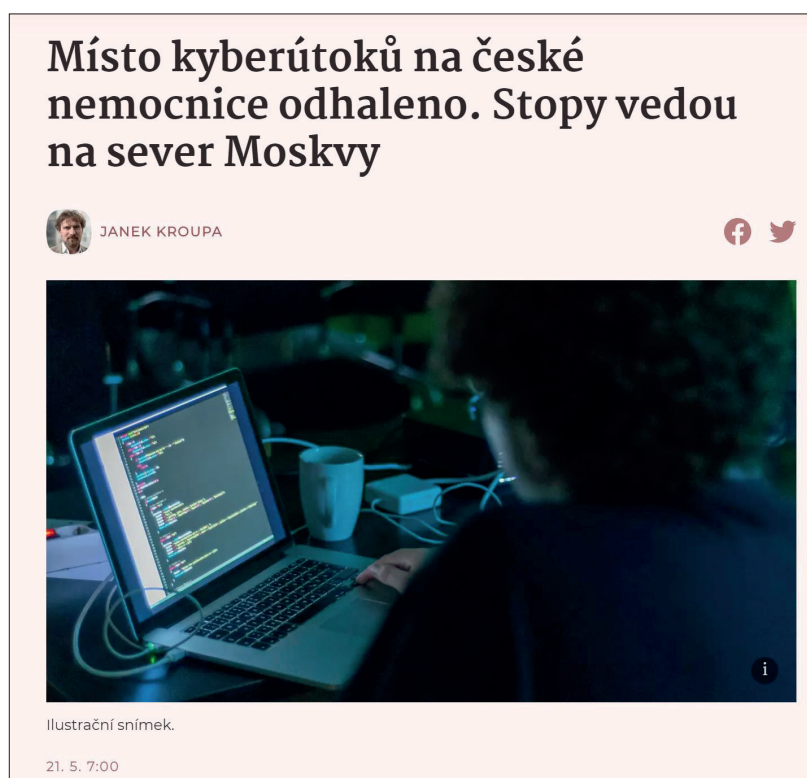
Махинации с «доказательствами» участия русских хакеров

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.

Рисунок 1. Скриншот публикации

(<https://www.seznamzpravy.cz/clanek/misto-kyberutoku-na-ceske-nemocnice-odhaleno-stopy-vedou-na-sever-moskvy-106710>)



Обвинения России в 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 появилась 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, также не объясняется.

Рисунок 3. Скриншот публикации

(<https://www.rmfm24.pl/fakty/polska/news-news-rmf-fm-za-falszywymi-alarmami-bombowymi-w-trakcie-zeszlorocznych-matur-std,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 об 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.

АНАЛИТИЧЕСКИЙ ОТЧЕТ

ИНФОРМАЦИОННАЯ ВОЙНА ПРОТИВ РОССИИ

ЧАСТЬ 1. КОНСТРУИРОВАНИЕ ОБРАЗА ВРАГА

Коллектив авторов:

Лемэр Лайма Германовна
Курицын Артем Николаевич
Семеновых Кристина Олеговна
Меликов Эмиль Эльбрусович

Дизайн и верстка:

Лебедева Наталья Владимировна

Формат:
60x90/8

Подписано в печать: 1 мая 2020 г.

Формат: 60x90/8

Тираж: 1500 шт.

Отпечатано: ООО «Красногорский полиграфический комбинат»

Адрес: 115093, г. Москва, Партийный переулок д.1, корп 58

Тел.: +7 495 374 98 90

E-mail: info@krpol.com



КРИБРУМ
Мы слушаем сеть

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



ИНФОРМАЦИОННАЯ ВОЙНА ПРОТИВ РОССИИ

ЧАСТЬ 1. КОНСТРУИРОВАНИЕ ОБРАЗА ВРАГА

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.