КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

«Экосистема безопасности российской национальной доменной зоны»

XX конференция «Обеспечение доверия и безопасности при использовании ИКТ»
23-24 марта 2022

круглый стол № 8



cctld.ru | кц.рф

.RU .РФ

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

УТВЕРЖДЕН
приказом Роскомнадзора
от 29.07.2019 № 216

**Перечень групп доменных имен,
составляющих российскую национальную доменную зону**

Российскую национальную доменную зону составляют доменные имена, входящие в следующие группы доменных имен, имеющих единое уникальное символьное значение (далее – домен верхнего уровня):

а) домен верхнего уровня .RU;

б) домен верхнего уровня .РФ;

в) домен верхнего уровня .SU;

г) иные домены верхнего уровня, управление которыми осуществляется зарегистрированными на территории Российской Федерации юридическими лицами, являющимися зарегистрированными владельцами баз данных указанных доменов в международных организациях распределения сетевых адресов и доменных имен.

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ (РОСКОМНАДЗОР)

ЗАРЕГИСТРИРОВАНО
Регистрационный № 55686
от 20 августа 2019

ПРИКАЗ

29.07.2019 Москва № 216

Об определении перечня групп доменных имен, составляющих российскую национальную доменную зону

.RU .РФ .SU

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

Безопасность DNS

Безопасность DNS:
- обеспечение целостности и доступности служб DNS,
- мониторинг активности DNS для определения возможных проблем безопасности в сети

Почему это важно?
- интересы государственной политики
- защита потребителя
- предупреждение преступности и атрибуция

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Злоупотребление DNS (DNS Abuse)

Вредоносная деятельность в Интернете

угрожает владельцам регистраций доменных имен и конечным пользователям за счет использования уязвимостей и функций экосистемы Интернета и DNS (протоколов, компьютерных систем, процессов регистрации доменов, пользователей и т. д.).

Эти угрозы включают такие действия, как:

- распределенные атаки типа «отказ в обслуживании» (DDoS)
- спам
- фишинг
- распространение вредоносное ПО (malware)
- управление вредоносным ПО (botnet controllers)
- Генерация доменов в автоматическом режиме (DGA)
- распространение незаконных материалов

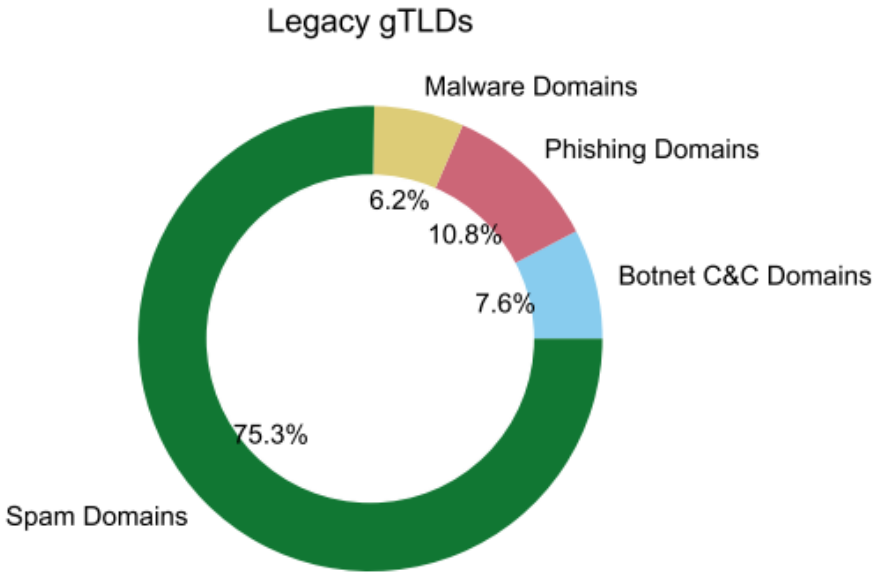
https://gac.icann.org/activity/dns-abuse-mitigation

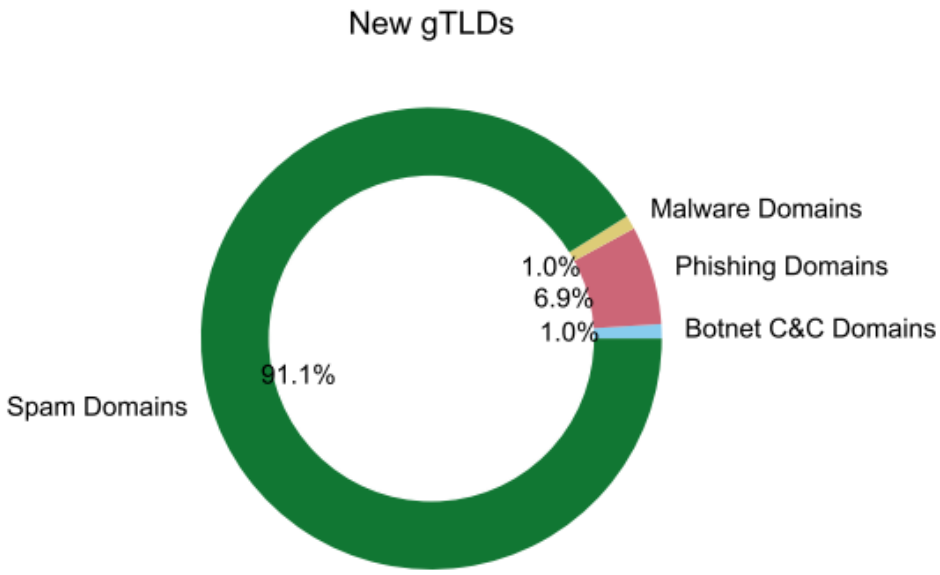


Грэм Бантон из DNS Abuse Institut: *DNS Abuse – это любой ущерб, который подвергает угрозе целостность DNS и совершается через DNS. Это может быть любое зловредное ПО Malwere, botnet, pharming, shiching*

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

ICANN DNS Abuse





По данным отчета ICANN Domain Abuse Activity Reporting (DAAR) за январь 2022
https://www.icann.org/en/system/files/files/daar-monthly-report-31jan22-en.pdf

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Мировые практики по борьбе с DNS Abuse

- Внедрение новых практик верификации пользователей, включая использование для авторизации и верификации государственные (системы национальных ID) и межгосударственные базы данных

- Мониторинг существующих ресурсов с целью оперативного выявления и пресечения деятельности противоправных ресурсов

- Развитие взаимодействия сторон (регистратуры, регистраторы, правоохранительные органы и экспертные организации) для оперативного пресечения злоупотреблений

- Внедрение раннего выявления системных регистраций, потенциально ассоциированных с противоправными ресурсами и злоупотреблениями DNS, в том числе с использованием искусственного интеллекта

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Проекты Координационного центра

Координационный центр доменов .RU/.РФ активно внедряет и поддерживает существующие практики и разрабатывает собственные уникальные механизмы, которые нередко переходят на уровень лучших мировых практик

Экосистема безопасности российской национальной доменной зоны

Доменный патруль рф

с 2012 года

Нетоскоп

с 2012 года

госуслуги

скоро…

институт компетентных организаций, а также: собственные методики мониторинга,
отраслевые мероприятие по обмену опытом,
резервирование системы регистрации,
образовательные мероприятия и многое другое

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Доменный патруль: институт КО



Новые компетентные организации:

Ростелеком Солар

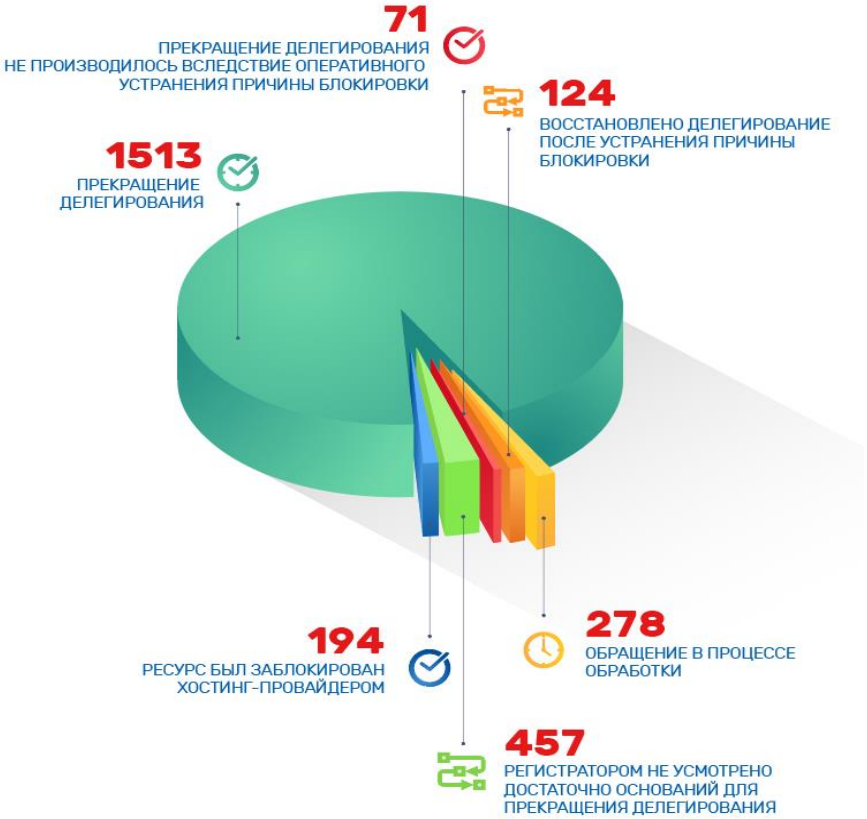
ФГУП МНИИ Интеграл

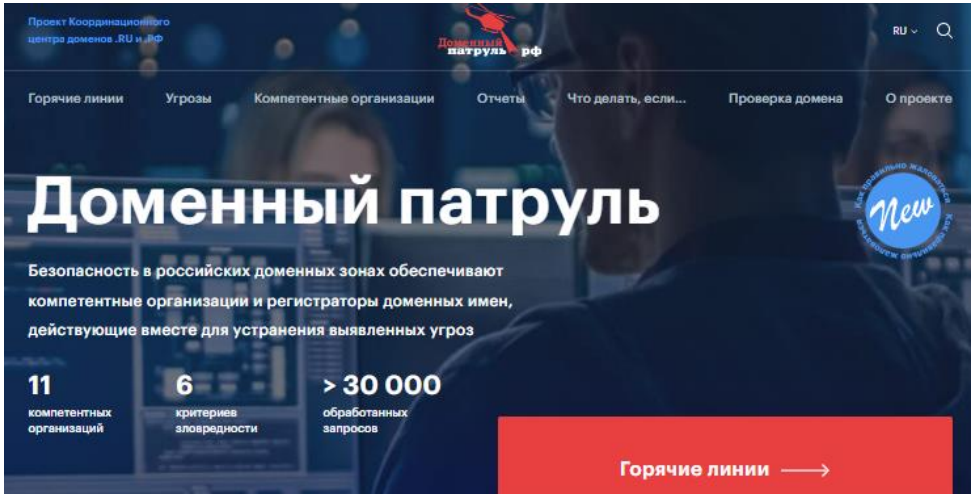
январь 2022г: **12** компетентных организаций

96 аккредитованных регистраторов

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Доменный патруль: итоги года





итоги 2021 года:

11 637 обращений, из них более **90% - фишинг**

92,0% - ресурс заблокирован (прекращено делегирование или сайт заблокирован провайдером)

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

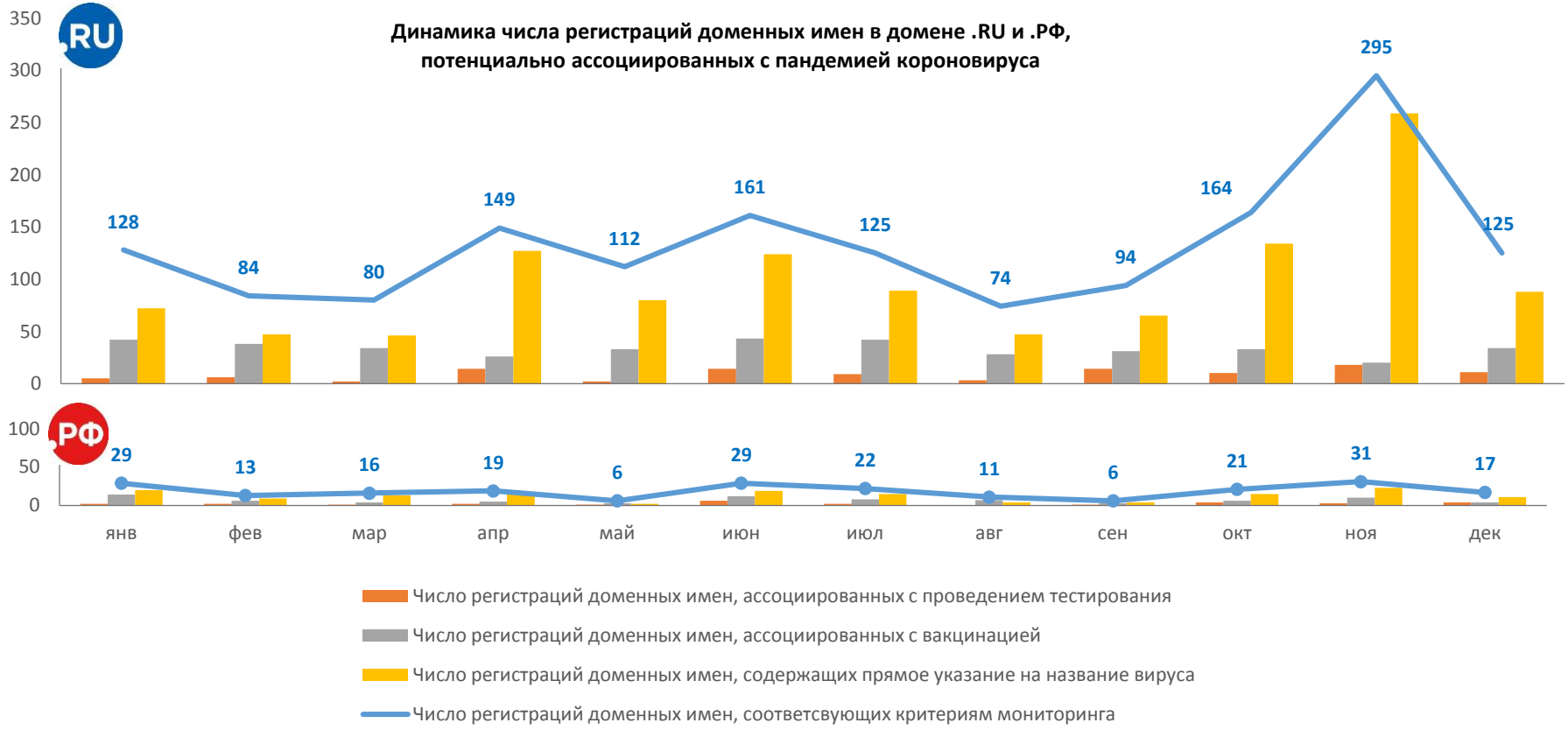
НЕТОСКОП



Участники научно-технического сотрудничества совместно развивают исследовательскую платформу для агрегации информации о вредоносных ресурсах в сети Интернет,
проводят анализ источников «зловредов» и обмениваются аналитическими

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Системы мониторинга



КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Другие элементы экосистемы

Обеспечению функционирования и эксплуатации резервной системы регистрации (договор с МСК-IX 16 марта 2021г.)

Резервная система регистрации предназначена для временного принятия на себя основных критических функций действующей системы регистрации доменных имен по решению регистратуры

- Режим готовности
- Режим повышенной готовности
- Режим объявления события
- Режим развертывания
- Режим стабилизации
- Режим завершения

Совершенствование Экосистемы безопасности —

это непрерывный процесс с вовлечением различных сторон от простых пользователей до экспертов по кибербезопасности и государства

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Минцифры России

Департамент развития инфраструктуры электронного правительства

Вопросы: о возможности присоединения информационных систем регистраторов доменных имен к Единой системе идентификации и аутентификации (далее — ЕСИА)

- Актуальный статус и перспективы присоединения информационных систем регистраторов доменных имен, аккредитованных АНО «Координационный центр национального домена сети Интернет», к Единой системе идентификации и аутентификации.
- Тенденции использования ЕСИА для идентификации и аутентификации организациями, отличными от финансового сектора и операторов связи. Какие типы организаций используют ЕСИА для идентификации и аутентификации в настоящий момент.
- Результаты эксперимента по подключению к ЕСИА сервисов агрегаторов объявлений.
- Динамика количества подтвержденных профилей пользователей ЕСИА физических лиц и юридических лиц

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

Мнение ведущих Регистраторов о присоединении информационных систем регистраторов доменных имен к Единой системе идентификации и аутентификации (далее — ЕСИА)

1. От АО РСИЦ Андрей Юрьевич Кузьмичев и Александр Николаевич Жгут,
2. от ООО Рег.ру Павел Андреевич Патрикеев.

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

GROUP IB

Мнение компетентных организаций о текущей ситуации и о присоединении информационных систем регистраторов доменных имен к Единой системе идентификации и аутентификации (далее — ЕСИА)

От Группы IB Александр Сергеевич Калинин

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

ТЦИ

ТЦИ является высокопрофессиональным техническим центром, который специализируется на поддержке DNS-инфраструктуры российского сегмента сети Интернет и взаимодействии с аккредитованными регистраторами. ТЦИ является сегодня технологической платформой для регистратур доменов верхнего уровня – Координационного центра доменов .RU/.РФ, РосНИИРОС (регистратура домена .SU), Фонда «Разумный Интернет» (регистратура домена .ДЕТИ), Координационного центра Регионального домена Республики Татарстан (регистратура домена .TATAR) – и работает с регистраторами доменных имен на уровне сервисных контрактов, оказывая им услуги по технической поддержке Главного реестра.

RIPE NCC (сетевой координационный центр)— это региональный интернет-реестр (RIR) для Европы, Ближнего Востока и некоторых частей Центральной Азии. Штаб-квартира находится в Амстердаме с филиалом в Дубае. RIR наблюдает за распределением и регистрацией ресурсов нумерации Интернета (адресов IPv4 , адресов IPv6 и номеров автономных систем) в конкретном регионе. RIPE NCC поддерживает техническую и административную координацию инфраструктуры Интернета. Это некоммерческая членская организация, насчитывающая более 10 000 членов, расположенных в более чем 76 странах региона обслуживания.

RIPE NCC Executive Board Resolution on Provision of Critical Services

At its meeting on 28 February 2022, the RIPE NCC Executive Board approved a resolution on provision of critical services.

The RIPE NCC provides critical services to its membership spread across a diverse geographical and political region.

The Executive Board of the RIPE NCC believes that the means to communicate should not be affected by domestic political disputes, international conflicts or war. This includes the provision of correctly registered Internet numbering resources.

The Executive Board of the RIPE NCC is committed to taking all lawful steps available to ensure that the RIPE NCC can provide undisrupted services to all members across our service region and the global Internet community.

The RIPE NCC will publicly document all its efforts to ensure that the registry is not negatively affected by laws, regulations or political developments.

It is crucial that the RIPE NCC remains neutral and does not take positions with regard to domestic political disputes, international conflicts or war.

This guarantees equal treatment for all those responsible for providing Internet services. This is a fundamental reason why the RIPE NCC has been able to maintain its operations in the way it has for the past three decades. It also means that the information and data provided by the RIPE NCC can be trusted as authoritative and free from bias or political influence. Failure to adhere to this approach would jeopardise the very model that has been key to the development of the Internet in our service region.

The Executive Board also expresses solidarity with those operators who have the difficult task of maintaining Internet access to assist the people suffering from the terrible effects of armed conflicts and war.

- *Publication date: 01 Mar 2022 — NEWS, NCC SERVICES*

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ



ICANN

2 March 2022

Mykhailo Fedorov
Deputy Prime Minister, Minister of Digital Transformation
Ukraine

Dear Deputy Prime Minister,

I am writing in response to your letter received 28 February 2022. First, let me express my personal concern for the well-being of your citizens in the midst of this conflict. ICANN and its global community are aware of and concerned about the terrible toll being exacted against your country.

You have asked that ICANN target Russia's access to the Internet by revoking specific country-code top-level domains operated from within Russia, arranging the revocation of SSL certificates issued within those domains, and shutting down a subset of root servers located in Russia.

ICANN is an independent technical organization that manages the Internet's unique identifiers. ICANN is a facilitator of the security, stability, and resiliency of these identifiers with the objective of a single, global, interoperable Internet. In our role as the technical coordinator of unique identifiers for the Internet, we take actions to ensure that the workings of the Internet are not politicized, and we have no sanction-levying authority. Essentially, ICANN has been built to ensure that the Internet works, not for its coordination role to be used to stop it from working.

As you know, the Internet is a decentralized system. No one actor has the ability to control it or shut it down. ICANN's primary role, through the functions of the Internet Assigned Numbers Authority (IANA), is to ensure the consistent and unique assignment of Internet identifiers in line with global policies. These policies were developed by a multistakeholder community that includes technical experts, businesses, academics, civil society, governments, and other stakeholders who worked collaboratively to solve policy and technical challenges through consensus. It is a model that has allowed the Internet to flourish over decades, and this broad and inclusive approach to decision-making fosters the global public interest and makes the Internet resilient against unilateral decision-making.

I want to specifically address your requests, from both the technical and policy perspective:

- For country-code top-level domains, our work predominantly involves validating requests that come from authorized parties within the respective country or territory. The globally agreed policies do not provide for ICANN to take unilateral action to disconnect these domains as you request. You can understand why such a system cannot operate based on requests from one territory or country concerning internal operations within another territory or country. Such a change in the process would have devastating and permanent effects on the trust and utility of this global system.

ICANN

- The root server system is composed of many geographically distributed nodes maintained by independent operators.
- We do not have the ability to revoke the specific SSL certificates for the domains you mentioned. These certificates are produced by third-party operators and ICANN is not involved in their issuance.

As you have said in your letter, your desire is to help users seek reliable information in alternative domain zones and prevent propaganda and disinformation. It is only through broad and unimpeded access to the Internet that citizens can receive reliable information and a diversity of viewpoints. Regardless of the source, ICANN does not control Internet access or content.

Within our mission, we maintain neutrality and act in support of the global Internet. Our mission does not extend to taking punitive actions, issuing sanctions, or restricting access against segments of the Internet – regardless of the provocations. ICANN applies its policies consistently and in alignment with documented processes. To make unilateral changes would erode trust in the multistakeholder model and the policies designed to sustain global Internet interoperability.

ICANN stands ready to continue to support Ukrainian and global Internet security, stability, and resiliency.

Sincerely,

Göran Marby
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers (ICANN)

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

RIPE NCC
RIPE NETWORK COORDINATION CENTRE



RIPE NCC Response to Request from Ukrainian Government

Letter from the Vice Prime Minister of Ukraine to RIPE NCC (PDF)
Response from Managing Director of the RIPE NCC (PDF)

Amsterdam, 10 March 2022

Dear Vice Prime Minister,

First, let me say that we at the RIPE NCC condemn the violent actions that have been taken against Ukraine and your people. Such actions undermine the cooperation that is at the heart of the Internet.

Your letter asks us to take four separate actions. Because our response to the first three will be of a more technical nature, we have addressed these in a separate appendix included with this letter. This is so we can provide you with a clear and straightforward response to your fourth request, which is the most relevant to our role and deserves the most attention: *"Withdraw the right to use IPv4 and IPv6 addresses by all Russian members of the RIPE NCC"*.

We regret to inform you that we cannot comply with this request. We do not have a mandate to take such actions, and as an organisation governed by community developed policy and Dutch law, we cannot take such action unilaterally. We further believe that Internet number resource registrations should not be used as a means to enforce political outcomes, and that doing so would have serious implications for the Internet, not just in the Russian Federation but also for the rest of the world.

We are the authoritative source of information on who holds the right to registration of IP addresses and ASNs in our service region. Internet operators use this registry to make their own decisions on how to route Internet traffic, resulting in an open Internet in which everyone can connect on their own terms. Blocking or withdrawing resources from our registry would be unlikely to have immediate impact on interconnection or traffic in Russia, but it could have unpredictable consequences in terms of harming the global coordination that is necessary for stable Internet operations.

This is an outcome that would play into the hands of those who want a less open Internet that can be used to enforce political decisions rather than allow open communications across the globe. As part of the technical community, we have long campaigned to maintain the open Internet, and our ability to do this depends heavily on preventing the registry from being used to achieve political ends.

Another effect of removing entries from our registry would be to diminish the ability of Internet operators to identify the source of Internet traffic, and consequently undermine their ability to make effective choices about who they should accept or block traffic from. Our registry also acts as an important data source for those who wish to monitor the health of the Internet in Ukraine and other countries. We provide this data freely to the Internet community and others who carry out research on the Internet and how traffic is routed over it. Compromising our registry in any way, or changing it according to political needs, would reduce trust in the data we provide and compromise everyone's ability to get clear insight and understanding of what is actually happening with the Internet at any given time.

Although we are unable to comply with your specific request, I want to give you our assurance that we will do everything we can to ensure our Ukrainian members remain able to provide services to your people. For example, we will be contacting Ukrainian members to make it clear that they do not risk losing their IP addresses if they cannot pay their invoices or are unable to comply with certain administrative requests. They carry out their work under the most difficult circumstances imaginable, and we wish to express our solidarity with them and our respect for their efforts to maintain Internet access at such a critical time.

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

К наиболее важным задачам организации относятся:

- Распределение и регистрация адресов IPv4 и IPv6 и номеров автономных систем (AS)
- Работа с базой данных RIPE
- Управление кластером серверов K-root, одним из 13 корневых серверов имен в мире.
- Содействие деятельности сообщества RIPE
- Развитие сети RIPE Atlas
- Предоставление качественных информационно-измерительных услуг

Finally, let me express my deep sympathy for the people of Ukraine and my sincere hopes for an end to the war that afflicts your country. We are a membership organisation, and we have close and long-held ties with many Ukrainian network operators who are providing Internet services to your people. And, crucially for us, we have Ukrainian staff among us, who experience great pain and uncertainty as they watch events unfold. With all of this in mind, I find it completely understandable that you would make this request of us. I only hope you can understand why it is that we must refuse.

Yours sincerely,

Hans Petter Holen
Managing Director
RIPE NCC

Appendix: Response to Remaining Items

Your letter requests four separate actions. For the sake of completeness, we have included our response to the remaining three below.

1. *Revoke, permanently or temporarily, the domains ".ru", ".рф" and ".su". This list is not exhaustive and may also include other domains issued in the Russian federation.*

The RIPE NCC does not have any role in issuing or revoking top-level domains like those you have listed. This remains the responsibility of ICANN and we refer you to their response.

2. *Contribute to the revoking for SSL certificates for the abovementioned domains.*

The RIPE NCC is not a Certificate Authority (CA) for domain names and does not issue SSL/TLS certificates for websites. The RIPE NCC is also not a member of the CA/Browser Forum.

3. *Disable DNS root servers situated in the Russian Federation, namely:*
4. *Saint Petersburg, RU (IPv4 199.7.83.42)*
5. *Moscow, RU (IPv4 199.7.83.42, 3 instances)*

The DNS root consists of 13 root servers operated by 12 independent organisations (including the RIPE NCC, which operates K-root). Aside from our underlying position as described in our accompanying letter, there is a strong consensus that the DNS must remain neutral. This can be seen in the following set of principles from the Root Server System Advisory Committee (RSSAC), which includes the principle that the root server system "must be a stable, reliable, and resilient platform for the DNS service to all users".

Publication date: 10 Mar 2022 — NEWS

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

СПАСИБО!

Андрей Воробьев a.vorobyev@cctld.ru

cctld.ru | кц.рф

.RU .РФ