Регистратуры доменных имен и онлайн-контент

Совет европейских национальных регистратур доменов верхнего уровня (CENTR)

Содержание

Основные положения

Члены Совета европейских национальных регистратур доменов верхнего уровня (CENTR) являются регистратурами национальных доменов верхнего уровня (ccTLD). В их обязанности входит предоставление и обеспечение работы технической инфраструктуры системы доменных имен (DNS) для соответствующих доменов верхнего уровня (TLD), организация процесса регистрации доменных имен, а также ведение баз данных регистратур, чтобы доменные имена могли использоваться при работе в интернете.

Оскорбительный и незаконный контент подрывает доверие к интернету как пространству инноваций, творчества и экономических возможностей. Регистратуры ccTLD принимают комплексные и эффективные меры по борьбе с незаконным онлайн-контентом.

Интернет – это совокупность взаимосвязанных компьютерных сетей по всему миру, взаимодействующих посредством уникальных числовых IP-адресов. Система доменных имен (DNS) функционирует как своего рода слой поверх IP-инфраструктуры. Доменные имена упрощают навигацию в интернете. Например, когда пользователь набирает доменное имя сайта, DNS сообщает устройству пользователя соответствующий IP-адрес, где находится контент данного сайта.

Чтобы обеспечить доступность контента в интернете, он должен храниться хотя бы на одном компьютере или сервере, подключенном к интернету. Чтобы удалить контент из интернета, нужно удалить его с хостингового устройства, либо отключить устройство от интернета.

Определение незаконного контента регулируется местным законодательством, и требования могут быть разными в зависимости от контекста. Местное законодательство определяет, кто имеет полномочия принимать соответствующее решение.

Удаление незаконного контента – единственный эффективный способ предотвратить доступ к этому контенту. Прямой доступ к контенту или устройству, на котором хранится контент, имеют две стороны: это лицо, публикующее контент, и хостинг-провайдер. В первую очередь следует обращаться к ним.

Если доменное имя используется для облегчения доступа к контенту, владелец доменного имени может быть провайдером контента и хостинга, либо может сообщить имя провайдера. Имя и контакты владельца домена можно найти через официальную базу данных регистратуры, в которой содержится информация обо всех доменных именах, зарегистрированных в конкретном TLD.

Если удалить незаконный контент из интернета невозможно (а это единственно эффективное решение), можно попытаться затруднить поиск этого контента или усложнить доступ к нему. Существуют различные методы «блокировки» интернет-контента на разных уровнях и с привлечением различных участников. Общим для всех этих методов, однако, является то, что контент остается доступным, и это может нанести непреднамеренный косвенный ущерб. Поэтому такие методы следует считать временной мерой и применять в экстренной ситуации или в случае, когда все другие методы результата не принесли. Одной из таких мер является блокировка или удаление доменного имени.

Местное законодательство определяет, какой контент является незаконным, кто обладает полномочиями для принятия мер и какие процедуры являются допустимыми. Соответственно, в разных странах существуют свои правила. Каждая регистратура национального домена предъявляет свои требования к тем, кто регистрирует доменные имена. Эти требования в сочетании с местным законодательством определяют политику регистратур и их инициативы, направленные на решение проблемы незаконного контента.

Как правило, такая политика учитывает специфику местного сообщества, соответствует местному законодательству и отвечает местным потребностям, и зачастую разрабатываются в консультации и сотрудничестве с другими заинтересованными лицами. Эффективные правила и успешный опыт одного национального домена верхнего уровня могут стать источником вдохновения для других регистратур. Тем не менее, необходимо помнить, что в силу местной специфики, простое копирование проекта или политики не гарантирует аналогичный позитивный результат. Более того, правила одного национального домена могут оказаться незаконными применительно к другому ccTLD.

В отношении незаконного контента регистратуры ccTLD, наряду с прочим, принимают следующие меры:

- Информирование пользователей и распространение информации.
- Информирование и тесное сотрудничество с властями и правоохранительными органами;
- Работа с базой данных регистратуры с целью повышения качества данных WHOIS о регистрантах может дать косвенный позитивный результат, так как маловероятно, что регистранты с преступными намерениями будут регистрировать доменное имя, используя свою реальную личную информацию.
- Разработка процедур для обмена регистрационными данными с третьими лицами в пределах местных нормативно-правовых требований в области неприкосновенности данных.
- Разработка процессов и процедур для реагирования на сообщения о подозрительном контенте. Данные процедуры объединяет то, что они применяются к ограниченному числу конкретных случаев с привлечением внешнего эксперта для оценки контента.

Введение

Члены CENTR занимаются управлением реестрами одного или нескольких национальных доменов верхнего уровня (ccTLD). В их обязанности входит предоставление и обеспечение работы технической инфраструктуры системы доменных имен (DNS) для TLD, организация процесса регистрации доменных имен, а также ведение баз данных регистратур, чтобы доменные имена могли использоваться при работе в интернете.

Члены CENTR уверены, что доверие к интернету и его безопасность чрезвычайно важны для того, чтобы он оставался пространством инноваций, творчества и экономических возможностей. Оскорбительный и незаконный контент подрывает доверие к интернету. Регистратуры и другие заинтересованные стороны разрабатывают и внедряют комплексные и эффективные меры борьбы против незаконного контента.

Цель и задачи

Совместные усилия и успешное сотрудничество требуют, чтобы заинтересованные стороны осознавали функции и роль друг друга и учитывали существующие ограничения. Цель данного доклада – рассказать о роли администратора национального домена верхнего уровня, его отношении к онлайн-контенту, рассмотреть различные меры и присущие им ограничения, а также четко разъяснить, какими полномочиями обладает регистратура в отношении незаконного онлайн-контента.

Структура

В первом разделе доклада рассказывается о том, как устроен интернет, где находится онлайн-контент, как можно получить к нему доступ, а также в чем заключается роль системы доменных имен (DNS).

Второй раздел доклада посвящен незаконному контенту в интернете и мерам, которые могут принимать администраторы национальных доменов для устранения нелегального контента.

В третьем разделе рассматривается политика и практика регистратур на современном этапе, рассказывается о том, как различные регистратуры ccTLD стремятся действовать в интересах местного сообщества и тем самым вносят свой вклад в борьбу с незаконным контентом.

Интернет, система доменных имен и онлайн-контент

DNS как часть инфраструктуры интернета

Интернет и IP-инфраструктура

Интернет представляет собой совокупность взаимосвязанных компьютерных сетей, которые образуют мировую коммуникационную систему. Межсетевой протокол (IP) – это метод или набор правил, по которым данные пересылаются через интернет с одного устройства на другое. Для успешной передачи важно, чтобы отправителя и получателя можно было распознать и найти среди миллионов компьютеров, смартфонов, серверов, устройств «интернета вещей» и других приборов, подключенных к интернету. Таким образом, каждое подключенное устройство имеет хотя бы один уникальный IP-адрес, который отличает его от других устройств. IP-адрес представляет собой числовой ярлык[1]: например, IP-адрес 2001:db8:85a3::8a2e:370:7334[2] указывает на интерфейс сервера, где хранится контент определенного сайта.

Система доменных имен

Людям сложно читать и запоминать числовые IP-адреса. Чтобы решить эту проблему, изобретена система доменных имен (DNS), которая позволяет использовать доменные имена для ссылки на IP-адреса. DNS является своего рода слоем поверх IP-инфраструктуры. Если, например, пользователь набирает доменное имя в строке браузера или нажимает на ссылку с доменным именем, устройство найдет в DNS соответствующий IP-адрес. Если доменное имя разрешится – то есть, DNS выдаст IP-адрес, то устройство пользователя будет знать, где в интернете можно найти контент определенного сайта или почтовый ящик, связанный с определенным электронным адресом.

DNS имеет иерархическую структуру, состоящую из различных доменов верхнего уровня (TLD) под одним корнем. Расширение доменного имени (после последней точки) указывает, под каким TLD зарегистрировано имя (например, .de, .com, .fr). Иерархическая структура необходима для функционирования DNS и циклического поиска доменных имен[3].

Регистратура доменных имен управляет одним или несколькими TLD. Все регистратуры должны соблюдать технические правила и требования DNS, но каждый TLD руководствуется собственными правилами. Если общие TLD (gTLD) должны соблюдать правила и процессы, разработанные сообществом ICANN, то национальные TLD (ccTLD) устанавливают свою политику в соответствии с потребностями своего интернет-сообщества.

---

1 Адреса в протоколе IPv6 состоят из 128 битов и представляют собой шестнадцатиричную цепочку. Адреса в более старом протоколе IPv4 состоят из 32 битов и выглядят как группы десятичных чисел, разделенных точками.

2 Данный IP-адрес представлен только в качестве примера и ни на что не ссылается (RFC 3849, IPv6, документационный префикс).

3 Подробнее о работе DNS: https://www.centr.org/education/the-dns.html

Онлайн-контент

Прежде чем контент попадет в интернет, его необходимо создать, разместить и сделать доступным. Данный раздел описывает процесс публикации контента, а также функции и обязанности участников[4].

Предоставление доступа к контенту

Провайдер контента

Провайдер контента передает в интернет текст, звук, изображения, видео, анимацию и другие виды контента, которые загружаются на сайт, публикуются в блоге, социальных сетях и т. д. Провайдер контента не обязательно является его создателем.

Чтобы контент стал доступен в интернете, он должен храниться хотя бы на одном компьютере или сервере, подключенном к интернету. Провайдер контента может использовать собственный компьютер или сервер, но чаще пользуется услугами и инфраструктурой хостинг-провайдера.

Хостинг-провайдер

Хостинг-провайдер предоставляет место для хранения и связь, обладает техническими знаниями и, что более важно, имеет необходимую инфраструктуру, мощности и пропускную способность для того, чтобы справляться с трафиком, который может прийти из любой части интернета в любое время. Хостинг-провайдеры предоставляют платформу для размещения контента, но не решают, что публиковать, а что нет. Такие решения принимают их клиенты (провайдеры контента). За редкими исключениями (крупные организации с собственной инфраструктурой и сетями) провайдер контента пользуется услугами хостинг-провайдера. Хостинг-провайдеры распоряжаются большими центрами обработки данных с серверами, на которых и хранится контент клиентов. Каждый сервер подключен к интернету и имеет уникальный IP-адрес. Существует несколько видов хостинга. Наиболее распространены веб- и email-хостинги. Хостинг соцмедиа (напр., пользовательские видео) можно считать особым случаем, средним между публикацией и хостингом.

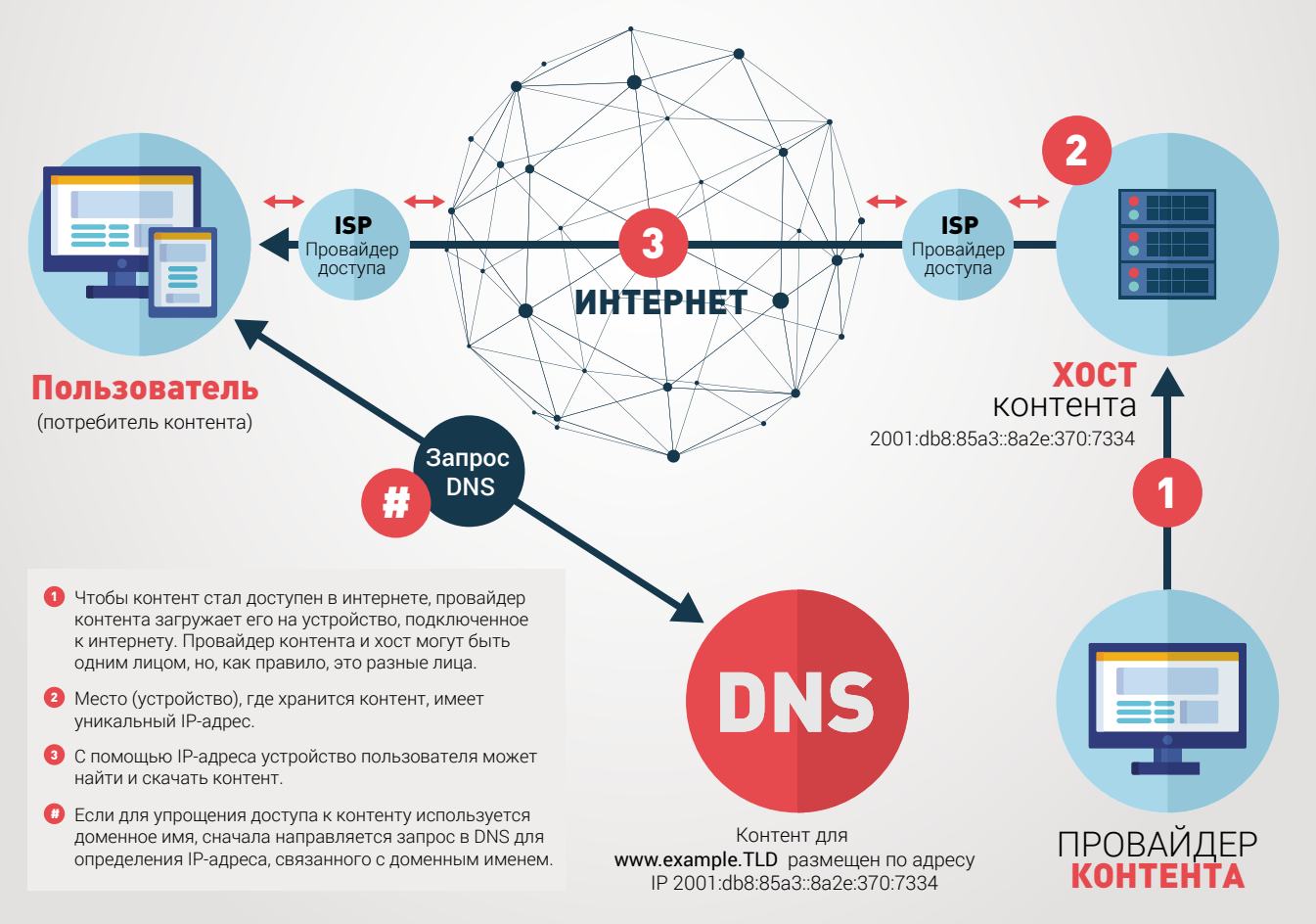
Провайдер интернет-услуг/провайдер доступа

Провайдер интернет-услуг (ISP) предоставляет доступ в интернет с помощью своей сети и инфраструктуры. ISP присваивает IP-адреса устройствам, подсоединенным к его сети – например, серверам хостинг-провайдера, модему интернет-пользователя и т. д. Предоставляя доступ, ISP не хранит контент, но контент проходит через его инфраструктуру.

Существуют и другие участники, которые обеспечивают передачу и обмен данными между сетями. Это точки обмена интернет-трафиком (IXP) и операторы коммуникационных сетей большой и малой протяженности – сетей доставки контента (CDN)[5], которые хранят копии контента клиентов на серверах в разных географических точках для оптимизации опыта конечного пользователя (например, Cloudflare). Их взаимодействие с контентом в данной работе не рассматривается.

4 Участники могут выполнять несколько функций, описанных в данном разделе. Например, ISP может также предоставлять услуги хостинга.

5 https://en.wikipedia.org/wiki/Content_delivery_network



Использование DNS в качестве инструмента для поиска контента

Система доменных имен (DNS) обеспечивает функцию «навигации» интернета, позволяет определять IP-адреса, связанные с доменными именами. Поэтому DNS иногда сравнивают с телефонным справочником или реестрами недвижимости и компаний[6].

Владелец доменного имени/регистрант

Провайдер контента может зарегистрировать доменное имя, чтобы упростить интернет-пользователям поиск своего контента. Доменное имя является «ярлыком» IP-адреса, легче запоминается, чем числовой IP-адрес и может содержать полезную информацию – например, название компании в электронном адресе или указание на содержание сайта в доменном имени сайта.

Владелец доменного имени не всегда является провайдером контента (или единственным провайдером), опубликованного под доменным именем. Например, порталы университетов, блог-платформы или социальные сети позволяют другим пользователям публиковать контент на сайте под одним и тем же доменным именем.

Владелец доменного имени или регистрант обладает правами на конкретное доменное имя. Чтобы получить эти права, лицо или компания регистрируют имя в регистратуре TLD, напрямую или через регистратора. Владелец домена несет ответственность за то, как используется его имя.

6 https://en.wikipedia.org/wiki/Domain_Name_System

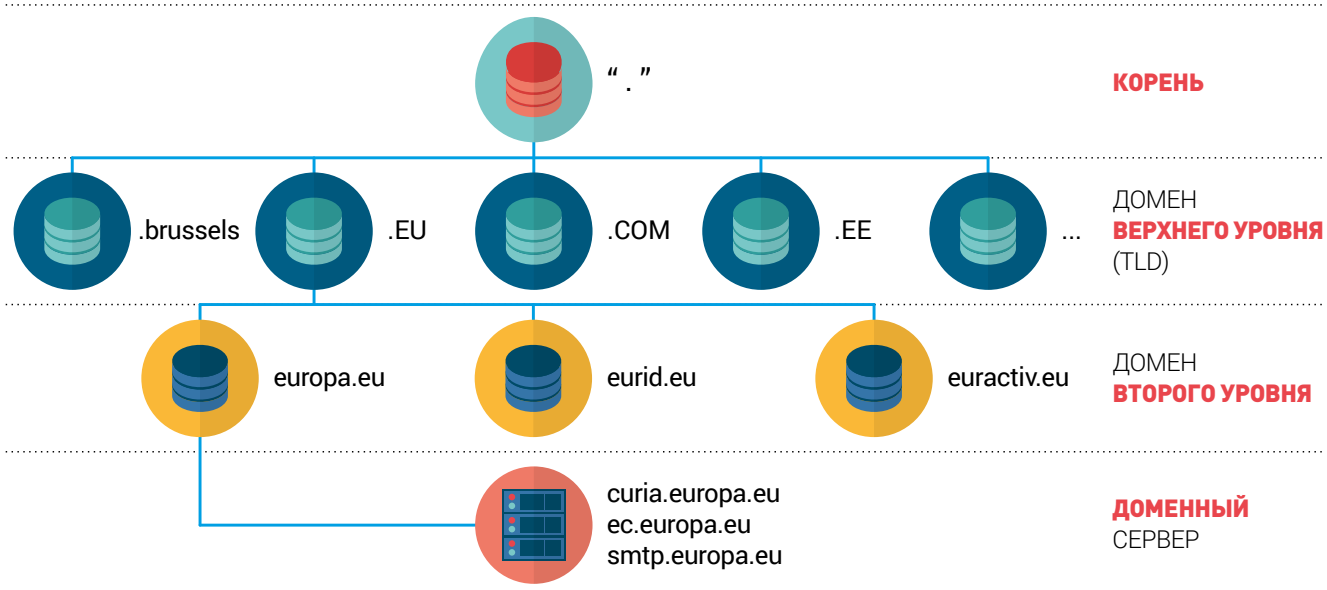
Регистратор доменного имени

Регистратор – это компания, которая предоставляет услуги регистрации доменов компаниям и физическим лицам, напрямую или через сеть реселлеров. Регистратор имеет аккредитацию одной или нескольких регистратур для предоставления доменных имен под их TLD. Регистратор проверяет доступность доменного имени и осуществляет процесс регистрации, в то время как регистратура управляет TLD запрошенного имени. В ходе процесса регистрации регистратор предоставляет контактную информацию владельца домена и техническую информацию касательно доменного имени (например, какие серверы имен содержат данные DNS, которые сообщат веб-браузерам и email-клиентам, где найти веб-сервер с контентом сайта или почтовый сервер электронной почты). Регистратор не хранит контент, и контент не проходит через его инфраструктуру. Тем не менее, на практике многие регистраторы также предоставляют своим клиентам услуги хостинга и другие услуги.

Администратор TLD

Регистратура управляет единственной официальной базой данных зарегистрированных доменных имен под своим TLD и публикует эту информацию в DNS. Серверы доменной регистратуры содержат информацию о владельце домена, регистрации домена (например, срок регистрации), IP-адреса, связанные с доменным именем, и другую техническую информацию. Регистратура несколько раз в день публикует обновленный файл зоны, который представляет собой текстовый файл – схему связи между доменным именем и его серверами имен для каждого зарегистрированного имени, а также другие ресурсы. Этот файл содержит информацию о том, как найти IP-адреса и другую информацию, необходимую для навигации в интернете. Регистратуры не хранят и не совершенствуют контент.

Примечание: Большинство ISP кэшируют информацию DNS о недавно запрошенных доменных именах из различных TLD на так называемые неофициальные серверы имен, чтобы ускорить процесс работы в интернете для своих клиентов. Запрос в DNS отправляют лишь в том случае, если в памяти сервера ISP нет упоминаний такого доменного имени. В результате внесение изменений в DNS (например, удаление доменного имени из DNS регистратурой) может занять некоторое время, прежде чем они распространятся на весь интернет.



Структура дерева DNS

Противодействие незаконному контенту в сети

Что такое незаконный контент?

Согласно местному законодательству

Термин «незаконный» используется для описания контента, который запрещен на государственном уровне, независимо от оснований. Например, Европейская комиссия дает такое определение: незаконный контент это «любая информация, которая противоречит законодательству Европейского союза или его государств-членов»[7]. Кроме материалов, связанных с сексуальным насилием против детей и растлением несовершеннолетних, в международном сообществе нет единства в вопросе о том, что считать законным контентом. Что разрешено в одной юрисдикции может быть запрещено в другой. Законность контента также может зависеть от контекста: признанный незаконным в одном контексте (например, просмотр непристойной комедии детьми), контент может быть приемлемым в другом (просмотр взрослыми) даже в пределах одной юрисдикции[8].

В некоторых странах существует специальное законодательство по онлайн-контенту. В других юрисдикциях вопросы онлайн-контента решаются на базе более общих законов, которые затрагивают не только интернет. По результатам сравнительного анализа, проведенного в 47 странах Совета Европы, были выявлены четыре категории правовых оснований для оценки онлайн-контента с точки зрения его законности:

- охрана здоровья и нравственности (включая детскую порнографию и незаконные азартные игры);
- обеспечение национальной безопасности, территориальной целостности и общественного порядка (включая контртеррористические меры);
- защита прав на интеллектуальную собственность; и
- защита от клеветы и неправомерного использования персональных данных[9].

Кто принимает решение о законности контента?

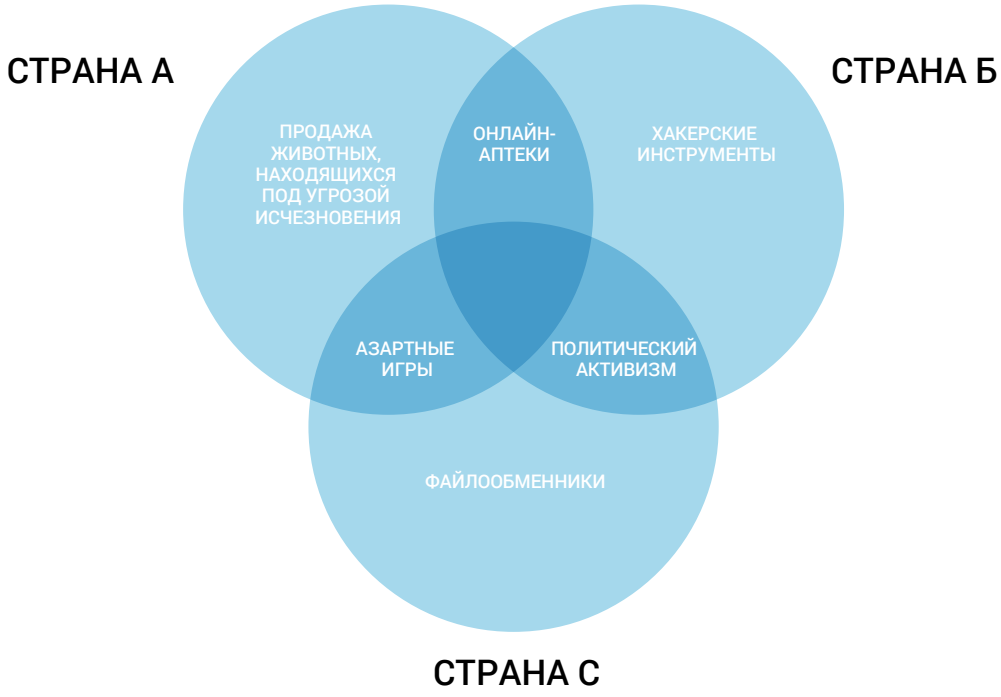
Определение незаконного контента регулируется местным законодательством. Кроме того, в зависимости от контекста один и тот же контент может быть признан как законным, так и незаконным. Незаконность контента определяет местный суд или компетентные органы. Более того, процедура может варьироваться даже в пределах одной юрисдикции. Некоторые органы власти могут обладать полномочиями для вынесения решения о законности контента и действовать напрямую исходя из этого решения, в то время как другие должны получить судебное решение для принятия мер.

---

7 *Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online,* C(2018)1177, European Commission, March 2018, https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegalcontent-online

8 *Internet Society Perspectives on Internet Content Blocking: An Overview,* Internet Society, March 2017, https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

9 *Comparative study on blocking, filtering and take-down of illegal Internet content,* CEO, December 2015, https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet (доступно по состоянию на 7 июня 2018 г.).



Как показывает диаграмма Венна, контент, являющийся законным в одних странах, может считаться вне закона в других.

Провайдер контента несет ответственность за контент, который он публикует для других интернет-пользователей. Владелец домена должен убедиться, что его доменное имя не используется для содействия доступу к незаконному онлайн-контенту. Ситуация может осложняться, если провайдер и пользователь находятся в разных юрисдикциях. Более того, сам контент может храниться в другом географическом регионе со своими законами, нормами морали и пониманием того, что законно, а что нет.

Когда дело касается онлайн-контента, регистратура ccTLD находится в том же положении, что и любая другая организация или даже физическое лицо. Регистратура может формировать мнение о том, что, по ее мнению, находится за рамками закона. У регистратуры нет особых полномочий для вынесения решений о законности контента, размещенного в интернете. Регистратура имеет точно такой же доступ к онлайн-контенту, что и любой пользователь, который заходит на сайт и загружает контент на свой компьютер. Не существует такого метода, который позволяет регистратуре узнать, какой контент публикует владелец домена. Регистратуры ccTLD не хранят контент, контент не проходит через их инфраструктуру.

Некоторые регистратуры могут предвидеть необходимость принятия мер в отношении очевидно противозаконного контента, когда сомнения практически отсутствуют и риск ответственности по их условиям минимален. Но в целом, регистратуры не обладают ни оборудованием, ни персоналом, ни полномочиями для того, чтобы заниматься поиском незаконного контента в интернете.

Где находится онлайн-контент?

Размещение в интернете

Чтобы пользователь получил доступ к контенту через интернет, контент должен храниться хотя бы на одном компьютере или сервере, подключенном к интернету. Расположение контента определяется уникальным IP-адресом или адресами устройства или устройств[10], на которых контент хранится.

10 Если быть технически точными, то IP-адрес присваивается интерфейсу, через который устройство передает информацию, а не самому устройству.

Фактическое местонахождение

Устройство или устройства, на которых хранится контент, могут находиться в любой точке мира, где есть электричество и интернет-соединение. Кроме того, с технической точки зрения не существует строгих правил или требований касательно того, где контент должен фактически храниться, хотя его фактическое местонахождение может повлиять на скорость и качество соединения.

Контент может храниться на одном или нескольких серверах (например, облачный хостинг, групповой хостинг). Контент может размещаться на одном или нескольких серверах в той же стране, где находится провайдер контента и его пользователь. Серверы также могут располагаться в любом другом месте и подчиняться правилам различных юрисдикций.

Удаление незаконного контента

Удаление незаконного контента – единственный эффективный способ перекрыть доступ к контенту и не допустить его употребление. Этого можно добиться путем удаления контента с устройства, на котором он хранится, либо отключив устройство от интернета.

Обращение к провайдеру контента или хостинг-провайдеру

Прямой доступ к контенту или устройству, на котором хранится контент, имеют провайдер контента и хостинг-провайдер. Провайдер контента обладает инструментами и кодами доступа, чтобы изменять или удалять контент, опубликованный на сайте, в соцсетях или где-либо еще. Хостинг-провайдер может удалить контент со своих серверов или заблокировать доступ к контенту через свою инфраструктуру.

Следует отметить, что хостинг-провайдеры обычно хранят контент разных клиентов на одном и том же устройстве, поэтому отключение или конфискация сервера может затронуть и других провайдеров контента, заблокировав доступ к законным материалам. Операторы соцсетей и блогов также имеют возможность удалять сомнительные публикации или незаконный контент, размещенный на их платформах.

Обращение к владельцу доменного имени

Владелец домена – это первое лицо, к которому следует обратиться, если доменное имя используется для обеспечения доступа к незаконному контенту. Владелец домена может одновременно быть провайдером контента, либо находиться с ним в тесном контакте. Владелец домена может не быть источником нелегального контента, либо не подозревать, что его доменное имя используется для распространения нелегального контента[11]. В большинстве случаев, владелец доменного имени способен помочь найти источник незаконного контента и предпринять шаги для его удаления.

Регистратура ведет официальную базу данных с информацией по всем доменным именам, зарегистрированным под ее TLD, и может помочь найти и связаться с регистрантом. База данных регистратуры, помимо прочего, содержит информацию о владельце домена, регистрации домена (например, срок регистрации) и адреса серверов имен, связанных с доменным именем.

Регистратуры ccTLD прикладывают большие усилия для того, чтобы поддерживать актуальность своих баз данных, и принимают обоснованные запросы на предоставление информации. Чтобы оперативно удалить незаконный контент из интернета, следует в первую очередь обратиться в регистратуру и получить информацию о владельце домена. Подробнее об этом – в разделе III о работе с регистратурами.

Примечание: Правоохранительные органы и другие органы власти могут получить в регистратурах дополнительную полезную информацию. Это могут быть данные по выставленным счетам и банковским картам, информация о других доменах, зарегистрированных тем же клиентом, и т. д.

11 Например, в случае порталов крупных университетов или социальных сетей, где множество пользователей публикуют свой контент и т. д., или если сервер взломан и используется преступниками для хранения контента.

Меры, призванные затруднить доступ к контенту

Если удалить нелегальный контент не удалось

Если не удалось найти провайдера или хостинг-провайдера контента или установить с ними контакт, чтобы удалить нелегальный контент, что является единственным действенным решением, можно попытаться усложнить доступ к этому контенту. Есть различные методы блокировки интернет-контента, на разных уровнях и с привлечением различных участников. В отчете Internet Society от 2017 года[12] описаны наиболее актуальные методы с оценкой эффективности каждого из них. В документе рассматриваются блокировка IP, блокировка на основе протокола, на основе технологии Deep Packet Inspection, на основе URL, на основе платформы и на основе DNS на уровне сети или ISP. В отчете сделан вывод о том, что, независимо от уровня и метода, «использование интернет-блокировки для борьбы с нелегальным контентом в целом нерационально, зачастую неэффективно и может привести к непредумышленному сопутствующему ущербу для интернет-пользователей». Блокировка контента не решает проблему: контент остается доступным, поэтому блокировку следует считать временной мерой и применять в экстренной ситуации или в случае, когда все другие методы результата не принесли.

В данном докладе речь пойдет о мерах, принимаемых на уровне доменной регистратуры, например, когда регистратура не позволяет доменному имени выдать действительный IP-адрес, временно заблокировав доменное имя или удалив его из зоны.

Риск и недостатки удаления доменного имени на уровне регистратуры

После блокировки или удаления доменного имени, то есть удаления его из DNS, пользователь больше не сможет получить действительный IP-адрес, если запросит доменное имя. Пользователь получит сообщение об ошибке, в котором будет сказано, что доменное имя не существует[13].

Удаление или блокировка доменного имени – довольно простая техническая операция, но предполагает серьезное вмешательство в DNS, в результате которого доменное имя больше не может использоваться для поиска контента (незаконного и законного), который публикуется под этим доменным именем и его различными поддоменами, а все сервисы, связанные с доменным именем (например, электронная почта), перестают работать. Обычно это происходит в течение нескольких часов, но из-за кэширования может занять и несколько дней. В любом решении удалить или заблокировать доменное имя необходимо учитывать все последствия, опираясь на здравый смысл и соразмерность данной меры. В Положении ЕС о сотрудничестве в защите потребителей (вступит в силу в январе 2020), например, четко говорится, что требовать от регистратур удаления доменного имени следует, только если «исчерпаны другие эффективные способы прекратить или запретить нарушение согласно данному Положению и чтобы избежать серьезного вреда коллективным интересам пользователей»[14].

Некоторые ccTLD, согласно местному законодательству и юрисдикции, сотрудничают с местными правоохранительными органами и/или авторитетными агентствами безопасности или компьютерными группами реагирования на экстренные ситуации с целью повысить доверие к ccTLD и их безопасность путем оперативного удаления или деактивации доменных имен, которые используются в преступных целях. Как правило, такое сотрудничество основано на том, что обе стороны понимают суть процессов и методов контроля, обеспечивая справедливость и обоснованность решений. Принимаемые меры зависят от нормативной базы в стране ccTLD, а также правовых вопросов и вопросов ответственности касательно уведомлений со стороны третьих лиц.

12 Internet Society Perspectives on Internet Content Blocking: An Overview, Internet Society, March 2017, https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

13 Domain Conflicts in the Legal System, Norid, September 2017, https://www.norid.no/en/domenekonflikter/rettslig-behandling/veileder/

14 Regulation (EU) 2017/2394 of 12 December 2017, entering into force 17 Jan 2020. Art.9, 4, (g), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R2394&from=EN

Ниже описываются некоторые риски и проблемы, связанные с блокировкой и удалением доменных имен.

Блокировка или удаление доменных имен может усложнить доступ к незаконному контенту в интернете, но не является решением этой проблемы, как и проблемы преступного деяния, поскольку контент остается доступным для тех, кто хочет его найти. Кроме того, существуют определенные риски и препятствия, о которых говорится ниже.

Сомнительный эффект и ложное чувство безопасности, поскольку контент остается доступным

Заблокировав или удалив доменное имя, мы не удаляем незаконный контент из интернета. Контент по-прежнему доступен напрямую через IP-адрес вместо доменного имени. Получить доступ к IP-адресу – задача нехитрая, и простым поиском в Google можно найти подробные инструкции и видео, объясняющие, как получить доступ к сайту через его IP-адрес. Удалив доменное имя, можно снизить шанс того, что пользователи случайно наткнутся на незаконный контент, но эта мера не остановит тех, кто намеренно его ищет. «Конечные пользователи могут легко обойти блокировку доменного имени, поэтому в долгосрочной перспективе эта мера неэффективна, а в ближайшей перспективе чревата непредвиденными последствиями»[15].

Более того, провайдеры нелегального контента, предвидя блокировку, могут принять соответствующие меры, чтобы ослабить ее эффект. Провайдер контента может, например, зарегистрировать несколько доменных имен в одном или нескольких TLD в разных юрисдикциях и сделать так, что они будут выдавать один и тот же IP-адрес, а значит, один и тот же контент. Гиперссылки в электронных письмах или ссылки, опубликованные на различных платформах или сайтах, могут приводить прямо на нужный IP-адрес без использования DNS.

Риск обширной блокировки и сопутствующий ущерб

Удаление или блокировка доменного имени влияет на весь контент, доступный под этим доменным именем или поддоменами, включая контент, подлежащий блокировке, а также прочий контент. Удаление доменного имени социальной сети или блог-платформы, где пользователи публикуют собственный контент или создают личный блог, влияет на всех пользователей – не только тех, кто публикует незаконный контент, но и тех, кто публикует семейные фотографии и комментирует политику, на компании, которые продвигают свой товар и используют сайт для электронной коммерции, и т. д. При блокировке доменного имени все сервисы, связанные с ним, например, электронная почта, тут же перестают работать.

На примере вымышленного кейса в исследовании «Конфликты с доменами и право» норвежская регистратура описывает последствия блокировки доменного имени Университета Осло после того, как студент опубликовал нелегальный контент в домене университета[16].

Риск злоупотреблений и ошибок

С технической точки зрения заблокировать доменное имя довольно просто, поэтому возникает риск злоупотреблений[17]. Для блокировщика цена ошибки невысока, однако эти действия могут нанести серьезный ущерб владельцу домена[18], например, если заблокирован сайт компании, занимающейся электронной торговлей, или перестала работать электронная почта в учреждении.

Примечание: Существуют другие способы блокировки и вмешательства в DNS – например, на уровне ISP или регистратора. Большинство из них связаны с теми же рисками, и эти меры так же можно обойти. Ни один из способов блокировки не является окончательным, так как ни один из них не удаляет контент.

15 I'SAC 056 - SSAC Advisory on Impacts of Content Blocking via the Domain Name System', SSAC, 9 October 2012.
16 См. текст в рамке на стр.10, Domain Conflicts in the Legal System, Norid, September 2017, https://www.norid.no/en/domenekonflikter/rettslig-behandling/veileder/
17 'Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation: (pp. 1379 - 1383)
18 Пример приводится в блоге: "Main French Internet Provider Orange blocks traffic to Google', Alix Guillard, 27.10.2016, https://en.blog.nic.cz/2016/10/27/french-orange-blocks-traffic-to-google/

Новейшие подходы национальных доменов верхнего уровня

Как говорилось ранее, местное законодательство определяет, какой контент является незаконным, кто обладает полномочиями принимать меры по борьбе с ним и какие процессы разрешены в рамках закона. В разных странах правила могут отличаться. Более того, регистратуры ccTLD формулируют свои требования касательно того, кто может регистрировать доменные имена и каковы их обязанности. Совокупность этих требований и местных законов влияет на политику и инициативы, которые разрабатываются регистратурами для борьбы с незаконным онлайн-контентом.

Как правило, эта политика тесно связана с нуждами местного интернет-сообщества, соответствует местному законодательству и разрабатывается в сотрудничестве с другими заинтересованными сторонами. Проведение эффективной политики и успешный опыт в рамках одного национального домена могут стать источником вдохновения для других участников. Однако, в силу местной специфики, нет гарантии, что простое копирование проекта или политики даст такой же позитивный результат или будет законным в юрисдикции другого ccTLD.

Информирование и обучение с упором на открытый диалог и сотрудничество с правоохранительными и другими государственными органами

Интернет-пользователи сталкиваются с различными рисками и угрозами (техническими, соблюдение конфиденциальности и т. д.), в число которых входит распознавание и предотвращение распространения незаконного контента. Некоторые регистратуры ccTLD считают своей обязанностью предупреждать сообщество об опасностях в интернете. Они обучают пользователей мерам защиты, рассказывают о способах снижения рисков и решения проблем.

Обучение и информирование интернет-сообщества

Регистратуры ccTLD занимаются информированием и обучением местных интернет-сообществ с целью повышения безопасности интернета. Регистратуры берут на себя инициативу предупреждать и просвещать владельцев доменов и широкую общественность о нежелательном контенте и дают рекомендации, как поступать в случае его обнаружения. Регистратуры информируют сообщества различными способами: например, организуют встречи или участвуют в мастер-классах, делают презентации, обсуждают вопросы незаконного контента в своих публикациях и т. д.

На сайтах многих регистратур есть страница или раздел о незаконном контенте, где говорится о возможных проблемах и угрозах, разъясняется политика регистратуры, ее роль и технические возможности в отношении незаконного контента.

Регистратура предоставляет необходимую информацию пользователям, которые желают подать заявление о потенциально незаконном контенте в организации и государственные органы, специализирующиеся на оценке и работе с конкретными видами онлайн-контента (например, незаконные азартные игры, детская порнография, контрафактные товары и т. д.).

Примеры

Nic.at (.at): сайт австрийской регистратуры с информацией о национальной службе по борьбе с детской порнографией и национал-социализмом в интернете. См. здесь и здесь.

Nominet (.uk): регистратура .uk объясняет, как пользователи, которые хотят заявить о неподобающем контенте, могут связаться с регистратором или владельцем сайта, и дает ссылки на британские органы власти, которые также могут помочь. См. здесь.

AFNIC (.fr): французская регистратура дает ссылку на специальную платформу Министерства внутренних дел, через которую можно заявить о «контенте сайта или поведении, которое противоречит закону и нарушает порядок».

Norid (.no): сайт норвежской регистратуры дает ссылку на сайт полиции и рекомендации, как сообщить в полицию о незаконной деятельности онлайн, а также ссылается на сервис slettmeg.no, разъясняющий, как удалить информацию из интернета.

DNS.PT (.pt): португальская регистратура в сотрудничестве с другими организациями, борющимися с нарушением авторских прав, создала портал, который обеспечивает простой и быстрый доступ к сайтам с цифровым контентом, опубликованный с соблюдением права авторов и создателей на интеллектуальную собственность.

Иногда регистратуры используют свои каналы коммуникаций, чтобы предупредить о работе мошенников, использующих поддельные сайты, например, с целью получения персональной информации пользователя для доступа в онлайн-банк или совершения покупок в интернете. Они также объясняют пользователям, как проверить подлинность сайта. Обычно поддельные сайты регистрируются под экзотичным TLD другой страны, и регистратура не имеет доступа к доменному имени и не может оказать на него никакого влияния.

Пример

Регистратура SIDN's (.nl) недавно опубликовала предупреждение о мошенничестве в онлайн-банках.

Обучение и тесное сотрудничество с правоохранительными органами

Многие регистратуры уделяют повышенное внимание информированию и установлению тесных контактов с правоохранительными и другими государственными органами (например, службами по защите прав потребителей или органами по борьбе с азартными играми). Важно, чтобы эти службы и органы, которые во многих случаях уполномочены оценивать легальность контента, понимали функцию регистратуры и ее возможности в плане борьбы с незаконным контентом. Важно выстроить эффективные каналы коммуникации. Тогда не придется терять время на то, чтобы просить регистратуру принять меры, которые она принять не может, вместо того чтобы адресовать запросы лицу или службе, которые имеют соответствующие полномочия. Правоохранительные органы играют важную роль в борьбе против незаконного контента онлайн. В большинстве случаев именно к ним следует в первую очередь обращаться с жалобами.

Важно, чтобы работники правоохранительных и других органов власти хорошо понимали, как устроены интернет и DNS, в том числе роль регистратуры, ее возможности и ограничения. Некоторые регистратуры также разрабатывают рекомендации или процедуры для выстраивания эффективных коммуникаций с соответствующими учреждениями, органами власти и регистратурой.

Примеры

Норвежская регистратура NORID (.no) подготовила руководство для правоохранительных органов, полиции и работников системы правосудия – «Конфликты с доменами и право». Кроме того, в сотрудничестве с прокуратурой, регистратура разработала отдельные инструкции для правоохранительных органов с описанием процедуры блокировки доменного имени.

SWITCH (.ch): В случае уголовного или административного разбирательства государственные органы могут направить в регистратуру запрос на аннулирование или блокировку доменного имени. В сотрудничестве с регулятором регистратура разработала рекомендации, где говорится, как действовать в таких случаях и какими полномочиями обладает SWITCH в плане исполнения предписаний органов власти.

Регистратура Nominet (.uk) в сотрудничестве с местным интернет-сообществом разработала процедуру сотрудничества с британскими правоохранительными органами. Согласно данной процедуре, британские правоохранительные органы могут представить Nominet официальное подтверждение преступного использования доменов .uk или незаконного контента на них, что приведет к временной блокировке в течение 48 часов после уведомления регистранта и регистратора. Отчет о временной блокировке публикуется ежегодно.

Регистратура как поставщик достоверных данных о доменном имени

Как говорилось выше, единственной эффективной мерой в борьбе с нелегальным контентом является удаление контента из интернета. Если пользователь или организация обнаружит нелегальный контент на каком-либо сайте, в первую очередь необходимо связаться с владельцем домена, который может удалить или изменить контент.

Регистратура собирает данные, чтобы иметь возможность определить владельца домена (ее клиента) и связаться с ним в случае спора, технических проблем, изменений в Условиях использования, пропущенных платежей и т. д. Условия использования обычно требуют от владельца домена предоставить корректные данные и контактную информацию в процессе регистрации и поддерживать эту информацию в актуальном состоянии. Предоставление ложной или некорректной информации является нарушением Условий использования и может привести к удалению доменного имени.

Регистратуры тратят много усилий и времени на поддержание своей базы данных. Это повышает качество регистрации данных в WHOIS и может дать косвенный позитивный результат, так как вряд ли кто-либо, имеющий преступные намерения, будет регистрировать доменное имя, указывая свои подлинные персональные данные. Методика поддержания высокого качества базы данных зависит от местного законодательства, размера регистратуры, количества обработанных регистраций и т. д. и может включать следующее[19]:

- тщательная проверка данных, предоставленных при регистрации, чтобы отфильтровать явно поддельные запросы (например, регистрантов по имени Микки Маус);
- автоматическая проверка формата предоставленных данных (например, электронного адреса и номера телефона);
- проверка юридических документов, представленных регистрантом, в странах, где такое требование предусмотрено законодательством;
- произвольная проверка регистрационных данных уже зарегистрированных доменных имен (например, регистратура случайным образом выбирает и проверяет определенное количество доменов в день, месяц или год);

19 Приведенные примеры основаны на опросе одного из участников CENTR в 2017 г.

- проверка данных в случае поступления жалоб;
- сверка предоставленных данных с официальными базами данных (например, актуальность почтового индекса, существование такого телефонного номера, проверка номера компании/организации или государственного идентификационного номера, если такая информация требуется в процессе регистрации).

Важно отметить, что многие регистратуры ccTLD напрямую с регистрантами никак не связаны. В этом случае все контакты, включая предоставление и актуализацию регистрационных данных, происходят через регистратора.

> **Примеры деятельности регистратуры для получения регистрационных данных и поддержания их в актуальном состоянии:**
>
> Регистратура Norid (.no) требует, чтобы все владельцы доменов были либо зарегистрированы в Норвежском центральном координационном реестре юридических лиц или в Государственном реестре. Администратор доменной зоны .no регулярно проверяет статус владельцев домена согласно Центральному координационному реестру юридических лиц. Домены юридических лиц, которые больше не существуют, удаляются.
>
> Регистратура DK Hostmaster (.dk) требует, чтобы датские регистранты предоставили свой NemID, специальный идентификационный аккаунт, который используют датские банки, правительственные сайты и некоторые частные компании. В отношении зарубежных регистрантов проводится процедура оценки рисков, по результатам которой регистранта просят представить удостоверение личности до регистрации, если риск высокий, или в течение 30 дней после регистрации, если риск низкий (при отсутствии риска подтверждение не запрашивается). Если владелец домена не может или не желает представить удостоверение личности, доменное имя удаляется.
>
> Регистратура SIDN (.nl) считает, что поддельные сайты портят репутацию .nl как надежного и безопасного домена верхнего уровня. Регистратура работает над системами раннего выявления доменов, которые используются для поддельных сайтов, изучает жалобы жертв мошенничества, а также информацию, полученную от Государственной службы оповещений об интернет-мошенничестве. Если регистрационные данные доменных имен связаны с поддельными сайтами, регистратура может их деактивировать.

Некоторые регистратуры разрабатывают специальные процедуры для выявления поддельных регистрационных данных:

- Nominet (.uk) направляет жалобы в случае обнаружения некорректных данных в WHOIS
- AFNIC (.fr) Verification запрашивает данные регистрантов
- DNSBelgium (.be) Revoke/Revoke+

Передача регистрационных данных третьим лицам

Регистратуры должны соблюдать правила сохранения конфиденциальности, принятые в своей стране, при передаче информации о владельцах доменов третьим лицам. Политика и процедуры получения контактной информации публикуются на сайтах регистратур. Различные регистратуры действуют по-разному. Некоторые просят вручную заполнить онлайн-форму, другие предоставляют доступ (ограниченный после вступления в силу «Общего регламента по защите данных») к регистрационной базе данных (через протокол Whois), третьи создают инструменты, с помощью которых можно направить сообщение напрямую регистранту.

Примеры

AFNIC (.fr): Запрос о раскрытии персональных данных

AFNIC (.fr): Связаться с официальным контактным лицом доменного имени

DomReg.lt (.lt): Связаться с регистрантом домена

Реагирование на сообщения о подозрительном контенте

Некоторые регистратуры разработали процедуры реагирования на сообщения о подозрительном контенте, которые блокируют или временно закрывают доступ к доменному имени. Эти процедуры объединяет то, что они применяются к ограниченному числу конкретных случаев с привлечением внешней стороны, специализирующейся на оценке такого контента.

Такие процедуры являются целесообразными, если судебное решение об отзыве доменного имени требует длительного времени. Недостатком таких процедур является то, что заявители не всегда осознают ограниченный характер мер, принятых регистратурой, и не предпринимает дальнейших усилий для удаления контентв из интернета.

Примеры

Регистратура SIDN (.nl) разработала добровольную процедуру «Увидеть и заблокировать», которая основывается на датском государственном своде правил под тем же названием. Процедура применяется только в тех случаях, если заявитель может доказать, что предпринял достаточно усилий, чтобы связаться с провайдером контента, менеджером сайта, регистрантом и регистратором доменного имени с целью решения проблемы и удаления контента. Только в случаях, когда налицо нарушение закона, SIDN может принять решение о (временном) удалении серверов имен для домена-нарушителя.

Switch (.ch) – статья 15 Постановления об интернет-доменах дает законные основания для блокировки доменных имен в случае «оправданных подозрений, что домен используется (1) для доступа к важным данным незаконными методами; или (2) для распространения зловредного программного обеспечения»; запрос на блокировку направляется службой по борьбе с киберпреступлениями, признанной швейцарским регулятором. См. здесь.

Finland (.fi) – статья 172 Закона о службах электронных коммуникаций предоставляет TRAFICOM право предпринимать необходимые действия для выявления, предотвращения и расследования существенных нарушений информационной безопасности, которые затрагивают публичные коммуникационные сети или службы и имеют отношение к доменным именам в национальном домене .fi или их владельцам. Такие действия могут быть направлены на данные корневого сервера имени .fi и могут включать следующее: 1) перекрытие и ограничение трафика на доменное имя; 2) перемаршрутизацию трафика на другой адрес; и 3) другие подобные технические меры по смыслу подпунктов 1-2.

Регистратура EURid (.eu) недавно заявила о сотрудничестве с Международной коалицией по борьбе с фальсификациями в целях очистки регистрационной базы данных для доменного пространства .eu и .ею от сфальсифицированных доменных имен и повышения безопасности доменного пространства для интернет-пользователей.

Заключение

Оскорбительный и незаконный контент подрывает доверие к интернету. Законодательство конкретной страны определяет, какой именно контент является незаконным и кто обладает полномочиями по борьбе с ним в рамках закона. В разных странах ситуация может отличаться.

Удаление незаконного контента из интернета – единственный эффективный способ, позволяющий перекрыть доступ пользователей к контенту. Провайдер контента и хостинг-провайдер имеют прямой доступ к контенту или устройству, на котором он хранится. Регистратуры ccTLD лишены доступа к контенту, не хранят его и не передают через свою инфраструктуру.

Регистратуры ccTLD вносят свой вклад в разработку эффективного всеобъемлющего подхода к решению проблемы незаконного онлайн-контента, разрабатывая соответствующую политику и инициативы, которые включают:

- информирование и просвещение интернет-сообществ в отношении опасности интернета;
- расширение сотрудничества с правоохранительными и другими государственными органами;
- предоставление регистрационных данных подозрительных доменных имен;
- реагирование на сообщения об использовании доменных имен для доступа к подозрительному контенту в соответствии с местным законодательством.

Приведенные в данном докладе эффективные меры и подходы могут стать источником вдохновения для других национальных доменов верхнего уровня. Тем не менее, в силу специфики каждой страны, нет гарантии, что копирование проекта или политики даст такой же позитивный результат или будет законно в юрисдикции другого ccTLD.

Совет европейских национальных регистратур доменов верхнего уровня (CENTR) – это ассоциация европейских регистратур национальных доменов верхнего уровня (ccTLD), таких как .de (Германия) или .si (Словения). В настоящий момент CENTR насчитывает 55 полных и 9 ассоциированных членов, в ведении которых находятся свыше 80% всех зарегистрированных доменных имен по всему миру. Задачей CENTR является участие в разработке и распространении высоких стандартов и передового опыта среди регистратур ccTLD.

Оцените данный доклад CENTR

(Благодарим за отзыв!)

CENTR vzw/asbl
Беллиардштраат 20 (6 этаж)
1040 Брюссель, Бельгия
Тел.: +32 2 627 5550
Факс: +32 2 627 5559
secretariat@centr.org
www.centr.org

Чтобы оставаться в курсе деятельности и докладов CENTR, следите за обновлениями в Twitter, Facebook или LinkedIn