RDAP vs WHOIS: вместе или вместо?

Автор: консультант по инфраструктуре
Координационного центра доменов .RU/.РФ
Вадим Михайлов

Термин WHOIS известен, пожалуй, каждому, кто когда-либо регистрировал для себя доменное имя. С помощью сервиса, основанного на этом протоколе, можно выяснить, существует ли домен в природе, кто является регистратором и регистрантом домена, когда домен создан и какой у него IP-адрес.

История WHOIS уходит корнями еще в середину 1970-х, когда Элизабет Фейнлер (Elizabeth J. Feinler) работала над каталогом ресурсов для ARPANET. Фейнлер вообще любила все систематизировать (ее первым проектом по систематизации еще в конце 1950-х годов стала индексация химических соединений), и ее исследовательская группа в 1974 году определила простой текстовый формат файла для имен хостов и несколько раз пересматривала формат по мере развития сетей. К 1982 году интернет-протокол для доступа к онлайн-справочнику людей, названный Whois (то есть «кто это»), приобрел свою окончательную форму и с тех пор изменялся лишь в отдельных деталях.

В начале 2000-х годов, одновременно с бурным развитием мирового доменного пространства, очевидной стала необходимость разработки более современного решения. В 2003 году в IETF велись разработки протокола CRISP – Cross Registry Information Service Protocol, который в дальнейшем был переименован в IRIS – Internet Registry Information Service. Однако, в 2013 году IETF пришлось признать, что протокол IRIS, в основном в силу своей технической сложности, не стал достойной заменой протоколу WHOIS.

Но IETF продолжила поиски решения, и в марте 2015 года рабочей группой Web Extensible Internet Registration Data Service (WEIRDS) был разработан протокол RDAP (Registration Data Access Protocol), который на данный момент описан в стандартах RFC 7480-7484, RFC 8521 и RFC 8056. Таким образом, сервис доступа к регистрационным данным наряду с WHOIS пополнился еще одним протоколом – RDAP.

В принципе, протокол RDAP выполняет те же функции, что и Whois. Основное отличие в том, что RDAP предоставляет возможность разграничения доступа к данным, и это особенно актуально сегодня в свете законодательно обусловленного крайне осторожного обращения с персональными данными пользователями. Например, можно сделать так, чтобы обычный интернет-пользователь получил доступ лишь к минимальной информации о доменном имени, а вот провайдеры, представители судов, адвокаты, правоохранители и все остальные категории пользователей, которым расширенный доступ необходим в силу служебных обязанностей, смогут получить тот объем данных, который соответствует их уровню доступа.

RDAP имеет ряд преимуществ перед WHOIS, ключевые из которых следующие:

- возможность использования авторизации и аутентификации

- корректная работа с интернационализированными данными
- функция поиска информации
- предоставление данных в машиночитаемом формате JSON
- поддержка SSL/TLS
- возможность расширения своих функций

Очень важно, что RDAP не требует внесения изменений в данные, которые уже хранятся и доступны с помощью протокола WHOIS. RDAP – это просто новый способ доступа к этим регистрационным данным.

Общий принцип взаимодействия клиента с сервером RDAP можно описать следующим образом: клиент направляет серверу HTTP-запрос, сформировав URL при помощи определенного в RFC 7482 набора RESTful-паттернов, а сервер отдает клиенту запрашиваемые данные в JSON-формате или возвращает код ошибки. В RDAP реализован подход, позволяющий получать данные не только по доменному имени или IP-адресу, но и по иным объектам при помощи <handle>-параметра с заданным оператором сервера синтаксисом.

Если нужен дифференцированный доступ к данным, RDAP позволит использовать аутентификацию и авторизацию клиентов в целях контроля и разграничения доступа к запрашиваемой информации. Аутентификация клиента возможна как стандартными методами HTTP протокола, определенными в RFC 7235, так и средствами TLS при помощи X.509 сертификатов. Работа в этом направлении продолжается, протокол RDAP достаточно гибкий, чтобы обеспечить поддержку дополнительных методов аутентификации, если возникнет необходимость в их использовании. Кроме того, ведутся разработки в сфере применения механизмов федеративной аутентификации для совокупности RDAP-серверов. Аутентифицированный клиент может быть авторизован на получение большего объема данных, чем анонимный клиент. В RDAP предусмотрены значения статусов объектов данных – private, removed и obscured, призванные помочь оператору сервера дифференцировать объем передаваемых данных в зависимости от полномочий клиента.

Сильный импульс в развитии и внедрении протокол RDAP получил именно из-за возможности разграничения уровней доступа к данным. Произошло это отчасти в связи с принятием в Евросоюзе «Общего положения о защите данных» (GDPR), которое серьёзно ужесточило требования к хранению и обработке персональных данных. Большинство регистратур отреагировали на введение этих требований тем, что убрали все персональные данные администраторов из данных предоставляемых посредством WHOIS. К сожалению, это привело к проблемам легитимного использования этих данных, например, правоохранительными органами, юридическими службами, экспертными организациями по борьбе с кибератаками и т.д., потому как персональные данные оказались недоступны сразу всем. Стала очевидна необходимость дифференцированного подхода, использования разных ролей, с разным уровнем доступа к данным, которую протокол WHOIS обеспечить не мог. Кроме того, еще в 2011 году правление корпорации ICANN приняло рекомендацию своего Консультативного комитета по безопасности и стабильности (SSAC) о необходимости провести оценку мер по замене протокола WHOIS, что послужило дополнительным импульсом в направлении

создания ему достойной замены. В ответ на принятое Евросоюзом в апреле 2016 года и вступившее в силу с мая 2018 года «Общее положения о защите данных» (GDPR) корпорация ICANN совместно с заинтересованным сообществом разработали и, в июле 2016 года, опубликовали RDAP-профиль для общих доменов верхнего уровня (gTLD), целью которого было обеспечить в первую очередь gTLD регистратуры и регистраторов техническими инструкциями по внедрению протокола RDAP. На текущий момент gTLD RDAP-профиль состоит из двух основных документов, первый из которых «RDAP Technical Implementation Guide», содержит в себе технические аспекты внедрения, второй же «RDAP Response Profile» описывает требования существующей нормативной базы и действующих политик.

В мае 2017 года правление корпорации ICANN выпустило резолюцию, утверждающую документ «Temporary Specification for gTLD Registration Data», в котором содержались как технические требования, так и требования по разработке необходимой документации, которые должны быть выполнены до внедрения регистратурой или регистратором сервиса RDAP.

27 февраля 2019 года корпорация ICANN разослала уведомление всем аккредитованным регистратурам и регистраторам общих доменов верхнего уровня с требованием внедрить у себя RDAP сервис до 26 августа 2019 года.

По данным ресурса rdap.org, в настоящее время 1197 регистратур доменов верхнего уровня реализовали сервис RDAP и анонсировали ссылки на авторитативные RDAP-сервера в IANA Bootstrap Service Registry for Domain Name Space, специальном реестре IANA доверенных серверов RDAP для доменных имен. Среди них 17 национальных доменов верхнего уровня на латинице, что составляет всего около 7% от общего числа латинских ccTLD. Обусловлено это тем, что на национальные регистратуры требование ICANN по внедрению RDAP не распространяется. Однако, первыми еще в начале 2017 года его внедрили как раз регистратуры национальных доменов Аргентины (.ar), Бразилии (.br) и Чехии (.cz), а ближе к концу 2017 года к ним присоединились такие общие домены как .com и .net.

В настоящее время инфраструктура сервиса RDAP активно развивается в различных направлениях. Ожидаются изменения gTLD RDAP-профиля в соответствии с новыми разрабатываемыми политиками, такими как рекомендации EPDP по внесению изменений в упомянутую выше спецификацию Temporary Specification for gTLD Registration Data. Эти рекомендации в данный момент находятся на рассмотрении правления ICANN. Готовятся изменения в соглашения об аккредитации ICANN регистратур и регистраторов общих доменов, касающиеся удаления требований к реализации WHOIS.

Также заинтересованным сообществом активно ведутся разработки различных прикладных программных решений как серверной части, так и клиентской. Есть среди них и проекты с открытым исходным кодом, например, серверное ПО DNSBelgium (https://github.com/DNSBelgium/rdap) и Red Dog (https://github.com/NICMx/rdap-server/). Наряду с серверными решениями, разработано и немало клиентского ПО для формирования запросов и отображения в человеко-читаемом виде ответов RDAP-серверов. Например, веб-клиент ICANN (https://lookup.icann.org/) или веб-клиент (https://client.rdap.org/) от CentralNIC,

к которым разработан и консольный клиент с открытым исходным кодом (https://github.com/gbxyz/rdapper). Кроме того, существуют и реализации RDAP-клиента в виде мобильных приложений, например, приложение от Viagénie для iOS (https://apps.apple.com/us/app/rdap-browser/id1473692572) и Android (https://play.google.com/store/apps/details?id=ca.viagenie.rdapclient).

Помимо клиент/сервер программных продуктов, ведется разработка инструментов, предназначенных для проверки соответствия RDAP-сервера gTLD RDAP-профилю. На данный момент, например, можно воспользоваться скриптом от CentralNIC (https://gitlab.centralnic.com/centralnic/rdap-conformance). Viagénie также может по запросу предоставить свою разработку – RDAP Server Conformance Testing Tool.

В свою очередь, Координационный центр доменов .RU/.РФ предоставляет сервис WHOIS+ (https://cctld.ru/service/plus/), предназначенный для поиска и проверки информации о доменном имени. В основе сервиса WHOIS+ лежит протокол RDAP, а также специально разработанный веб-клиент, интегрированный с сервисом проверки доменного имени от компании «Онлайн Патент». Воспользоваться сервисом WHOIS+ может любой желающий, доступ к нему не ограничен. С помощью него можно узнать русскоязычные названия организаций, являющихся регистратором или администратором домена, в том случае если администратор юридическое лицо, а также информацию о наличии товарных знаков, совпадающих с доменным именем, и прочую информацию о нем. Подробнее о сервисе WHOIS+ можно прочитать здесь: https://cctld.ru/service/trademark/

Поскольку RDAP более современный протокол, обладающий куда более широкими возможностями, чем протокол WHOIS, а общий вектор систем предоставления данных стремится к машиночитаемым форматам, то можно предположить, что RDAP рано или поздно вытеснит WHOIS из широкого применения. Однако этот процесс займет немало времени, и еще долго сервисы доступа к регистрационным данным будут поддерживать протокол WHOIS, а у большинства регистратур будут поддерживаться и оба этих протокола.