Итоговый отчет экспертной рабочей группы по вопросам справочных служб рДВУ:

служба каталогов регистрации следующего поколения (СКР)

СТАТУС ДОКУМЕНТА

Настоящий документ представляет собой итоговый отчет экспертной рабочей группы по вопросам справочных служб рДВУ (ЭРГ) с подробным изложением наших рекомендаций Правлению ICANN относительно службы каталогов регистрации рДВУ следующего поколения (СКР), которая должна заменить сегодняшнюю систему WHOIS.

I. СВОДНАЯ ИНФОРМАЦИЯ

В настоящем итоговом отчете экспертной рабочей группы по вопросам справочных служб рДВУ (ЭРГ) подробно изложены наши рекомендации президенту/генеральному директору и Правлению ICANN относительно службы каталогов регистрации рДВУ следующего поколения (СКР), которая должна заменить действующую систему WHOIS.

Настоящий итоговый отчет представляет собой кульминацию интенсивной работы в течение более 15 месяцев, за время которой многообразная группа добровольцев потратила тысячи часов на всестороннее исследование, рассмотрела больше 2600 страниц комментариев общественности, полученные в ходе опроса ответы и результаты исследования, а также приняла участие в 19 открытых консультациях с сообществом, потратила 35 дней на очные совещания ЭРГ, провела 42 теле-конференций ЭРГ, более 200 телеконференций подгрупп и несметное количество заседаний с целью сбора комментариев сторонних экспертов и членов сообщества — и все это, чтобы ответить на простой вопрос:

Существует ли альтернатива сегодняшней системе WHOIS, которая лучше отвечает потребностям мирового интернет-сообщества?

Да, существует. ЭРГ единогласно рекомендует отказаться от сегодняшней модели WHOIS, предоставляющей каждому пользователю одинаковый совершенно анонимный открытый доступ к (зачастую неточным) регистрационным данным рДВУ.

Взамен ЭРГ рекомендует изменить существующую парадигму в пользу СКР следующего поколения, которая осуществляет сбор, проверку и раскрытие регистрационных данных рДВУ только в разрешенных целях.

Хотя основные данные останутся общедоступными, доступ к остальной их части будет предоставлен только аккредитованным инициаторам запросов, которые подтвердят свою личность, сообщат о своей цели и согласятся нести ответственность за ненадлежащее использование.

На следующих 150 с лишним страницах описаны полученные сведения и проведенные исследования, которые повлекли за собой эту рекомендацию ЭРГ, подробное предложение о создании новой СКР и следующие выводы и результаты:

- Этот вопрос очень сложный.
- ЭРГ изучила данный вопрос с множества ракурсов и провела исследование, чтобы обеспечить осуществимость предлагаемой СКР.

- Предлагаемая СКР, хотя и не является совершенной, отражает тщательно продуманные и сбалансированные компромиссы между взаимозависимыми компонентами, которые на следует разделять.
- Предлагаемая СКР предназначена для прямого и беспрецедентного разрешения:
    - трудных вопросов конфиденциальности данных;
    - трудностей проверки, которые долгое время ухудшали качество и точность данных; и
    - достижения реального равновесия между доступом и ответственностью.
- СКР необходимо внедрить как одно целое. Внедрение некоторых, но не всех, принципов проектирования, рекомендованных в настоящем документе, сведет на нет преимущества ее использования для всей экосистемы.

Настоящий итоговый отчет, в том числе включенные в него рекомендации и предлагаемые принципы построения СКР следующего поколения, отражает общее мнение. Этот факт заслуживает внимания, учитывая широкий спектр точек зрения и заинтересованных сторон среди участников ЭРГ.[1]

ЭРГ уверена, что настоящий итоговый отчет выполняет указание Правления ICANN содействовать переопределению цели и способов предоставления данных о регистрации рДВУ, создавая фундамент, на котором сообщество ICANN (через Организацию поддержки родовых имен — ОПРИ) выработает новую глобальную политику в отношении справочных служб рДВУ.

ЭРГ уверена, что описанная в настоящем итоговом отчете СКР создает более прочный фундамент, чем тот, который существует сегодня, — фундамент, на котором ОПРИ может выработать новую глобальную политику для регистрационных данных рДВУ, чтобы защитить неприкосновенность личной жизни и обеспечить увеличение точности, подотчетности и прозрачности всей экосистемы ICANN на годы вперед.

ЭРГ рекомендует при рассмотрении настоящего итогового отчета Правлением, ОПРИ и сообществом ICANN выстраивать обсуждение на основе следующих вопросов:

[1] Для получения сведений о составе ЭРГ и квалификации ее членов см. Приложение J.

- Является ли СКР более предпочтительной, чем сегодняшняя система WHOIS?
- Если нет, согласно ли сообщество ICANN с тем, что существующая система WHOIS должна продолжать работу и может удовлетворить потребности развивающегося мирового Интернета?

История вопроса

ЭРГ была сформирована генеральным директором ICANN Фади Шехаде (Fadi Chehadé) по просьбе Правления ICANN, чтобы облегчить разрешение тупиковой ситуации, существующей в рамках сообщества ICANN на протяжении почти десятилетнего периода и связанной с заменой существующей системы WHOIS.[2]

С целью преодолеть недостатки WHOIS, выявленные в многочисленных сообщениях и исследованиях сообщества[3], перед ЭРГ была поставлена задача пересмотреть и заново определить цели сбора и сопровождения регистрационных данных рДВУ, рассмотреть способы защиты данных и предложить систему следующего поколения, которая будет лучше отвечать потребностям глобального интернет-сообщества.

Начав с чистого листа, ЭРГ поставила под сомнение фундаментальные постулаты в отношении назначения, вариантов применения, сбора, сопровождения и предоставления регистрационных данных. ЭРГ рассмотрела каждую заинтересованную сторону, связанную со справочными службами рДВУ, изучив ее потребности в плане точности, доступа и конфиденциальности. Она обсудила возможные способы более эффективного удовлетворения этих потребностей.

Чтобы определить направление своих дискуссий, ЭРГ составила общее заявление о целях и использовала его для согласования рекомендаций настоящего отчета с миссией ICANN и проектирования системы, поддерживающей регистрацию и обслуживание доменных имен, которая:

[2] См. https://www.icann.org/news/announcement-2-2012-12-14-en

[3] Для ознакомления со списком сообщений, в которых документально зафиксированы недостатки WHOIS см. Приложение B.

- предоставляет необходимый доступ к точным, надежным и единообразным регистрационным данным;
- защищает конфиденциальность сведений о владельцах регистраций;
- создает надежный механизм идентификации владельцев регистраций, создания и сохранения возможности связываться с ними;
- поддерживает структуру, предназначенную для решения проблем с участием владельцев регистрации, включая, помимо прочего, защиту потребителей, расследование киберпреступлений и защиту интеллектуальной собственности; и
- создает инфраструктуру для удовлетворения законных потребностей правоохранительных органов.

Пользователи и цели

ЭРГ изучила существующие и потенциальные цели сбора, хранения и предоставления регистрационных данных рДВУ широкому спектру пользователей, проанализировав широкое репрезентативное множество примеров использования WHOIS.

ЭРГ рассмотрела весь набор примеров использования и накопленный в результате этого опыт, а также справочные материалы и комментарии сообщества, чтобы определить консолидированную совокупность пользователей и разрешенных целей, которая должна поддерживаться СКР, а также потенциальные злоупотребления, которые необходимо предотвратить.

Разрешенные или запрещенные цели использования

В соответствии с кругом обязанностей ЭРГ, все эти пользователи были изучены для определения существующих и возможных будущих рабочих процессов и участвующих в них заинтересованных сторон.

Были проанализированы потребности в информации о регистрации доменных имен, чтобы получить обязательный набор элементов данных, сопутствующих рисков, последствий для законов и политики в отношении непри косновенности личной жизни, и ответить на другие вопросы, изученные в настоящем отчете.

Справа в обобщенном виде представлены цели, которые ЭРГ рекомендует разрешить.

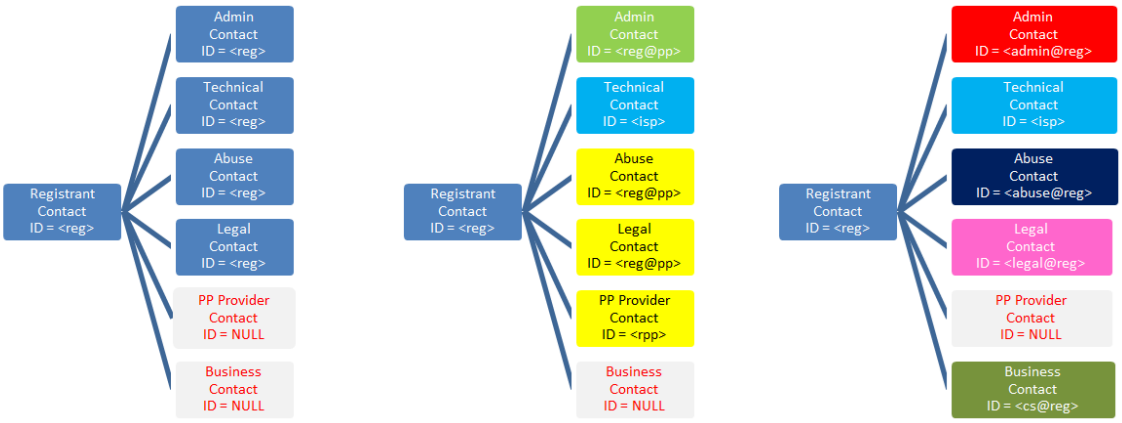
Выявленные на настоящий момент разрешенные цели и соответствующие потребности в плане регистрационных данных, контактов и запросов определены ниже и более подробно рассматриваются в разделе III.

Цель	Предусматривает такие задачи, как...
Управление доменным именем	Создание, управление и текущий контроль над доменным именем, принадлежащим владельцу регистрации (ДИ), в том числе создание ДИ, обновление информации о ДИ, передача ДИ, продление срока регистрации ДИ, удаление ДИ, сопровождение портфеля ДИ и обнаружение мошеннического использования собственных контактных данных владельца регистрации.
Защита персональных данных	Идентификация аккредитованного поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц или ответственного за утверждение защищенных учетных данных, связанных с этим ДИ, и направление такому поставщику информации о злоупотреблениях, запросов на раскрытие сведений, или установление иных контактов с этим поставщиком.

Цель	Предусматривает такие задачи, как...
Решение технических проблем	Работа над решением технических проблем, связанных с использованием доменного имени, включая проблемы доставки электронной почты, ошибки разрешения в DNS, а также функциональные проблемы веб-сайтов, путем установления связи с техническим персоналом, который отвечает за решение этих проблем.
Сертификация доменного имени	Необходимость подтверждения центром сертификации (ЦС), выдающим сертификат X.509 субъекту, определяемому доменным именем, того, что данное ДИ зарегистрировано на имя субъекта сертификата.
Индивидуальное использование Интернета	Идентификация организации, использующей доменное имя, для внушения доверия потребителям или установления связи с этой организацией с целью отправки претензий потребителей или подачи жалоб на эту организацию.
Покупка или продажа доменного имени в деловых целях	Отправка запросов на покупку ДИ, приобретение ДИ у другого владельца регистрации и обеспечение возможности проведения юридической экспертизы.
Исследование DNS в научных или общественных интересах	Изучение в научных или общественных интересах доменных имен, сведения о которых опубликованы в СКР, включая общедоступную информацию о владельце регистрации и назначенных им контактных лицах, историю и состояние доменного имени, а также сведения о доменных именах, зарегистрированных конкретным владельцем.
Юридические действия	Расследование возможного мошеннического использования принадлежащего владельцу регистрации имени или адреса другими доменными именами, расследование возможного нарушения прав на торговые марки, установление связи с законным представителем владельца регистрации/лицензии перед юридическим действием и последующее юридическое действие, если проблему не удается разрешить удовлетворительным образом.
Принуждение к соблюдению нормативных и договорных обязательств	Расследование налоговыми органами деятельности компаний, имеющих представительства в Интернете, расследование в рамках ЕПРД (UDRP), расследование соблюдения договорных обязательств и аудиторские проверки депонирования регистрационных данных.

Цель	Предусматривает такие задачи, как...
Расследование уголовных дел и предотвращение злоупотреблений в DNS	Передача информации о злоупотреблениях лицу, которое может расследовать и устранить данное злоупотребление, или установление связи с организациями, имеющими отношение к доменному имени, во время обычного расследования уголовных дел.
Прозрачность DNS	Отправка запросов на получение регистрационных данных, опубликованных владельцами регистраций, для удовлетворения широкого спектра потребностей широкой общественности в информации.

Чтобы обеспечить целевой доступ к регистрационным данным и одновременно улучшить связь и неприкосновенность личной жизни, ЭРГ разработала принципы использования целевых контактных лиц (ЦКЛ). С опорой на установленные роли и обязанности ЦКЛ были поставлены в соответствие всем разрешенным целям, для которых необходимо установление контакта. Ниже приведены три примера, которые подробнее рассматриваются в разделах III и IV.



Кроме того, ЭРГ проанализировала все элементы регистрационных данных, — начиная с тех, которые определены в CAP 2013, — чтобы получить набор руководящих принципов сбора и раскрытия данных, точно соответствующий рекомендованной концепции ЦКЛ, а также рекомендациям по обеспечению соблюдения законов о защите данных. ЭРГ также дала дополнительные рекомендации по определению новых элементов данных, которые владельцы регистраций и контактные лица, возможно, пожелают опубликовать для повышения надежности связи. Эти рекомендации подробно изложены в разделе IV, а в Приложении E приведены примеры.

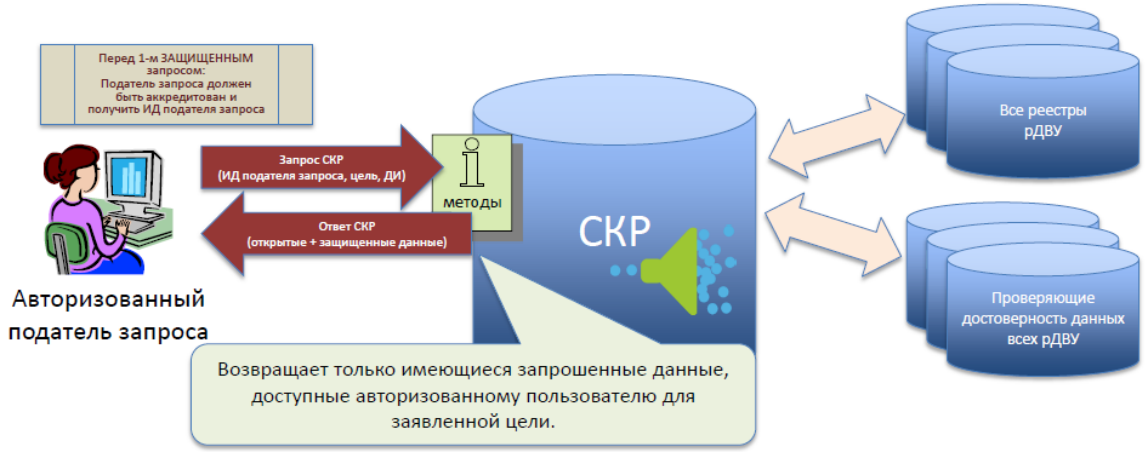
Целенаправленный доступ

Для рекомендованной СКР используется подход с чистого листа, который предусматривает отказ от универсальной модели WHOIS в пользу целенаправленного доступа к проверенным данным с надеждой на улучшение конфиденциальности, точности и ответственности. ЭРГ считает, что эта новая парадигма доступа способна повысить ответственность всех сторон, участвующих в раскрытии и использовании данных о регистрации доменных имен рДВУ, благодаря следующему:

- учет всего доступа к регистрационным данным рДВУ, в том числе доступа без проверки подлинности к открытым элементам данных, чтобы обеспечить обнаружение и устранение злоупотреблений;
- регулирование доступа к более конфиденциальным элементам данных, когда доступ предоставляется только тем инициаторам запросов, которые подали заявку и были аккредитованы в качестве лиц, имеющих право доступа к СКР, на уровне, подходящем для каждого пользователя и заявленной цели доступа; и
- аудиторские проверки как открытого, так и регулируемого доступа к данным для минимизации злоупотреблений и наложение штрафов и других санкций за ненадлежащее использование, в соответствии с условиями и положениями, принятыми в явном виде каждым инициатором запросов.

Разработанные ЭРГ принципы доступа к данным, которые легли в основу развернутых рекомендаций относительно открытого и регулируемого доступа к данным, изложены в разделе IV. Как изображено ниже, открытые элементы данных могут быть по-прежнему запрошены из СКР любым лицом, прошедшим или не прошедшим проверку подлинности.

Защищенные элементы данных тоже можно запрашивать через СКР. Для этого инициатор запроса сначала должен быть аккредитован. После этого инициаторы запросов могут отправлять заверенные запросы на получение элементов данных для заявленной цели.



В Приложении E более подробно описаны элементы данных, которые можно получить в ответ на открытые и авторизованные запросы данных, зависимость процедуры авторизованного доступа от пользователя и цели, а также роль, которую могут играть органы аккредитации пользователей СКР в авторизации и аудиторской проверке регулируемого доступа.

Защита конфиденциальности и данных

Центральным в круге обязанностей ЭРГ является вопрос о том, как разработать систему, повышающую точность собранных данных и одновременно предлагающую средства защиты тем владельцам регистраций, которые стремятся защитить и сохранить свою конфиденциальность.

ЭРГ признает, что личная информация защищена законами о защите данных и даже в отсутствие соответствующего законодательства у частных лиц есть законные причины стремиться к повышению защиты своей личной информации. Кроме того, некоторые компании и организации могут стремиться к защите своей информации для законных целей, например, на этапе подготовки к началу производства новой линейки продуктов или, в случае малого бизнеса, когда контактная информация содержит личные данные.

Соответственно, чтобы обеспечить регулярное соблюдение законов о защите конфиденциальности и данных, ЭРГ сформулировала набор рекомендаций, которые подробно изложены в разделе VI. Эти принципы охватывают следующее:

- механизмы, способствующие повседневному законному сбору данных и их передаче между участниками экосистемы СКР;
- стандартные пункты договоров, которые приведены в соответствие с законами о защите конфиденциальности и данных и закреплены в составе политики;
- «обработчик правил» для применения законов о защите данных; и
- взаимосвязь мест хранения данных СКР с доступом правоохранительных органов.

Помимо конфиденциальности, обеспечиваемой в соответствии с законами о защите данных, в составе СКР также рекомендованы принципы, которые учитывают потребности в конфиденциальности путем включения в состав экосистемы СКР:

- услуг сохранения конфиденциальности/регистрации через доверенных лиц для общего использования; и
- аккредитованных услуг защиты учетных данных для использования лицами, которые подвергаются опасности, а также в условиях лишения права на свободу слова или преследования мнений.

Кроме того, ЭРГ рекомендует ICANN изучить возможность выработки единой гармонизированной политики соблюдения конфиденциальности, обеспечивающей всестороннее регулирование деятельности СКР.

Для удовлетворения потребностей в более единообразных и надежных услугах сохранения конфиденциальности и регистрации через доверенных лиц, улучшающих подотчетность, ЭРГ включила в состав своих принципов ЦКЛ средства связи с поставщиками этих услуг. Она также рекомендовала принципы и концепцию сохранения конфиденциальности/регистрации через доверенных лиц в качестве исходных данных для рабочей группы ОПРИ по вопросам аккредитации служб сохранения конфиденциальности и регистрации через доверенных лиц.

Для удовлетворения потребностей частных лиц и групп, которые могут продемонстрировать, что окажутся под угрозой в случае их идентификации по регистрационным данным, ЭРГ рекомендует концепцию защищенных учетных данных, позволяющую указанным лицам анонимно подавать заявки и получать зарегистрированные доменные имена с использованием защищенных учетных данных при содействии органов аттестации и доверенных третьих лиц, создающих защитный экран между находящимися под угрозой субъектами и регистраторами.

ЭРГ рекомендует ICANN способствовать созданию независимой заслуживающей доверия ревизионной комиссии, которая будет осуществлять проверку заявлений организаций или частных лиц о том, что они подвергаются риску, для утверждения (и в необходимых случаях аннулирования) учетных данных.

Качество данных

ЭРГ рекомендует повысить надежность проверки представленных владельцами регистраций данных, которые предусмотрены в сегодняшней системе WHOIS или с учетом ее возможной модернизации благодаря широкому внедрению CAP 2013. К минимально необходимым улучшениям качества данных относятся следующие.

- Предоставление контактных данных владельцев регистраций на основе цели доступа должно привести к существенным улучшениям доступности надлежащих контактных лиц для различных целей и стимулировать владельцев регистраций к предоставлению точной информации о лицах, выполняющих данные роли.
- При использовании регулируемого доступа к более конфиденциальным элементам данных у владельцев регистраций будет меньше побудительных причин предоставлять неточные данные, вкупе с большей ответственностью за обеспечение точности данных.

Кроме того, ЭРГ рекомендует два смежных, но независимых улучшения:

- Стандартное подтверждение всех регистрационных данных рДВУ с использованием как периодических проверок, так и подтверждения в момент сбора данных, с возможностью блокирования неоднократного использования контактных данных для регистрации нескольких доменных имен до их подтверждения, а также с возможностью для пользователей СКР увидеть последние подтвержденные данные и степень их подтверждения; и
- Предварительно проверенный каталог контактных данных, принципиально независимый от каталога доменных имен, для содействия качеству и возможности неоднократного использования элементов данных, используемых для связи с владельцами регистраций и людьми или организациями, которые могут быть назначены владельцами регистраций в качестве ЦКЛ для различных целей, связанных с регистрацией доменных имен, и для ограничения мошеннического использования личных данных.

Принципы и процедуры, детализирующие данные рекомендации, можно найти в разделе V.

Модели реализации

При обсуждении путей реализации этих принципов и рекомендаций на практике ЭРГ изучила во всех подробностях несколько альтернативных моделей. Для оценки всех моделей использовалась совокупность разносторонних критериев, которые описаны в Приложении F. После тщательного анализа ЭРГ сделала следующие выводы.

- Сегодня регистраторы или аффилированные с регистраторами лица собирают и хранят регистрационные данные, полученные от своих клиентов (владельцев регистраций). Этот процесс по своей природе является распределенным. Помимо продолжения накопления регистраторами или аффилированными лицами регистрационных данных, предоставленных владельцами регистраций, ЭРГ предлагает осуществлять сбор контактных данных силами проверяющих.
- Существует множество возможных моделей хранения регистрационных данных всей совокупности рДВУ. ЭРГ выявила несколько возможных моделей, заострила внимание на двух, которые признала наиболее многообещающими, и рекомендует выбрать одну из них на основе критериев оценки.
- В интересах защиты конфиденциальности субъектов данных, централизованный интерфейс должен позволять надлежащим инициаторам запросов получать доступ к регистрационным данным всей совокупности рДВУ, включая нерегулируемый доступ к открытым данным и доступ к закрытым данным на основе авторизации.
- СКР должна использовать RDAP или EPP (в зависимости от интерфейса в каждом случае) в качестве основного протокола доступа к каталогу для получения регистрационных данных из мест хранения, где бы они ни находились.

ЭРГ разработала и проверила несколько альтернативных моделей системы, которые подробно описаны в Приложении F, в том числе модели, предложенные сообществом ICANN. Эти возможные модели отличаются друг от друга способом копирования или запроса регистрационных данных в СКР. ЭРГ тщательно изучила каждую модель, чтобы определить влияние этих различий. Сравнив указанные возможные модели, ЭРГ пришла к выводу, что все они, кроме нынешней системы WHOIS, в той или иной степени могут соответствовать принципам СКР, рекомендованным ЭРГ. ЭРГ выбрала среди этих моделей для дальнейшего изучения две наиболее многообещающие — интегрированную модель и синхронизированную модель (ранее известную как «агрегированная модель»).

Чтобы получить дополнительные данные для своего анализа, ЭРГ поручила нейтральной третьей стороне (IBM) выполнить анализ стоимости моделей реализации с целью определения необходимых условий и потенциальных

расходов для этих двух моделей. На основе выполненного ЭРГ углубленного анализа, а также представленного IBM отчета о результатах анализа, в результате которого выяснилось, что интегрированная модель является более затратной в масштабе всей экосистемы СКР, **в конечном итоге ЭРГ рекомендовала использовать синхронизированную СКР (ССКР).**

Заключение

По причине большой детализации, сложности и объема итогового отчета, настоящее сводное резюме на является всеобъемлющим обзором, и читателям рекомендуется обращаться за дополнительной информацией к основному тексту итогового отчета.

ЭРГ передала настоящий итоговый отчет генеральному директору ICANN и Правлению, открыто опубликовала его в Интернете и проведет несколько открытых консультаций с общественностью на лондонской конференции ICANN в июне 2014 года. Она также проведет интернет-семинары и предоставит другие возможности для обсуждения этого отчета и получения сообществом ICANN ответов на касающиеся отчета вопросы. Настоящий итоговый отчет должен создать фундамент для процесса разработки политики (ПРП) ОПРИ по запросу Правления в отношении предоставления регистрационных данных рДВУ и проведения в установленном порядке необходимых переговоров по условиям договоров.

ЭРГ уверена, что настоящий итоговый отчет выполняет указание Правления ICANN содействовать переопределению цели и способов предоставления данных о регистрации рДВУ, и создаст фундамент, на котором сообщество ICANN (через ОПРИ) выработает новую глобальную политику в отношении справочных служб рДВУ.

II. Полномочия, цель и результаты ЭРГ

а. Полномочия

Экспертная рабочая группа по вопросам справочных служб рДВУ (ЭРГ) была сформирована генеральным директором ICANN Фади Шехаде по просьбе Правления ICANN, чтобы облегчить разрешение тупиковой ситуации, существующей в рамках сообщества ICANN на протяжении почти десятилетнего периода и связанной с заменой существующей системы WHOIS. Несколько опубликованных за этот период отчетов и исследований сообщества[4] указывают на недостатки существующей системы, для устранения которых необходимо найти решение.

Задача ЭРГ состоит в том, чтобы пересмотреть и заново определить цели сбора данных и сопровождения справочных служб рДВУ, рассмотреть способы защиты данных и предложить систему следующего поколения, которая будет лучше отвечать потребностям глобального интернет-сообщества. Группа начала работу с чистого листа, изучив и подвергнув сомнению истинность фундаментальных постулатов в отношении назначения, вариантов применения, сбора, сопровождения и предоставления регистрационных данных. ЭРГ рассмотрела каждую заинтересованную сторону, связанную со справочными службами рДВУ, изучив ее потребности в плане точности, доступа и конфиденциальности, а также возможные способы более эффективного удовлетворения этих потребностей.

б. Цель

Для помощи в проведении обсуждений ЭРГ разработала следующее общее заявление о целях, исходя из которых она проверяла свои заключения и рекомендации:

> В поддержку миссии ICANN по координированию глобальной системы уникальных идентификаторов Интернета и обеспечению стабильного и безопасного функционирования системы уникальных идентификаторов Интернета необходимо, чтобы информация о доменных именах рДВУ способствовала доверию к Интернету со стороны всех заинтересованных сторон.

[4] Для ознакомления со списком сообщений, в которых документально зафиксированы недостатки WHOIS см. Приложение B.

Соответственно, желательно разработать систему для поддержки регистрации и обслуживания доменных имен, которая:

- Предоставляет необходимый доступ к точным, надежным и единообразным регистрационным данным
- Защищает конфиденциальность персональных данных
- Создает надежный механизм идентификации владельцев регистраций, создания и сохранения возможности связываться с ними
- Поддерживает структуру, предназначенную для решения проблем с участием владельцев регистрации, включая, помимо прочего, защиту потребителей, расследование киберпреступлений и защиту интеллектуальной собственности
- Создает инфраструктуру для удовлетворения законных потребностей правоохранительных органов

в. Результаты

24 июня 2013 года ЭРГ опубликовала свой первоначальный отчет, ответы на часто задаваемые вопросы и онлайн-анкету опроса, а затем начала процесс широких консультаций с сообществом ICANN по своим предварительным рекомендациям. В своем первоначальном отчете ЭРГ пришла к выводу, что от сегодняшней модели WHOIS, предусматривающей предоставление всем пользователям одинакового публичного доступа к (зачастую неточным) регистрационным данным рДВУ, следует отказаться. Взамен ЭРГ рекомендовала изменить существующую парадигму в пользу сбора, проверки и раскрытия регистрационных данных рДВУ только в разрешенных целях с предоставлением доступа к некоторым элементам данных тем инициаторам запросов, личность которых удостоверена и которые впоследствии будут нести ответственность за их правомерное использование.

ЭРГ сформулировала эту рекомендацию после всестороннего рассмотрения прошлых отчетов, в которых подробно рассмотрены недостатки WHOIS и множество различных заинтересованных сторон, использующих сегодняшнюю систему WHOIS. Для каждой выявленной группы пользователей ЭРГ проанализировала цели получения регистрационных данных и индивидуальные элементы данных, которые необходимы для этих целей. На основе данных этого анализа ЭРГ рекомендовала принципы и определила характерные особенности, с учетом которых должна создаваться служба каталогов регистрации следующего поколения (СКР). Чтобы проиллюстрировать возможные пути реализации этих

принципов, ЭРГ также рассмотрела несколько альтернатив и предложила модель сбора и раскрытия точных элементов регистрационных данных доменных имен для разрешенных целей.

11 ноября 2013 года, после тщательного рассмотрения всех полученных от сообщества ICANN комментариев и отзывов ЭРГ опубликовала отчет о текущем состоянии дел, в котором сделала упор на мнении ЭРГ по многим ключевым вопросам. По запросу сообщества, отчет о текущем состоянии дел также содержал намного более подробную информацию относительно анализа, который лег в основу первоначального отчета.

ЭРГ выполнила подробный анализ полученных отзывов о двух своих отчетах, используя обширный и многообразный вклад сообщества как исходные данные для своей текущей работы над нерешенными вопросами, а также для проверки и уточнения своих рекомендаций. Вследствие сложности решаемой задачи и важности того, чтобы в основу любой СКР следующего поколения легло твердое понимание ее вероятных преимуществ и последствий, ЭРГ провела исследование в пяти областях: сложившаяся практика подтверждения данных в нДВУ и коммерции, сложившаяся практика оказания услуг сохранения конфиденциальности и регистрации через доверенных лиц, изучение организаций, способных осуществлять аккредитацию пользователей СКР, и анализ рисков, выгод и издержек СКР. Результаты этого исследования, опубликованные в марте 2014 года, были использованы для дальнейшего уточнения рекомендаций ЭРГ.

На данный момент ЭРГ тщательно рассмотрела предыдущую работу над системой WHOIS, существующих и возможных будущих пользователей регистрационных данных рДВУ и их цели, комментарии множества разнообразных заинтересованных сторон относительно сегодняшней системы WHOIS, сложившуюся практику, связанную с предлагаемыми улучшениями СКР, а также выполнила анализ рисков, выгод и издержек СКР. Все эти данные были учтены в рекомендациях ЭРГ[5] относительно системы следующего поколения, которая подробно описана в настоящем итоговом отчете для Правления ICANN и предназначена для целенаправленного использования в процессе разработки политики.

[5] В этом отчете для принципов ЭРГ используются следующие понятия, основанные на определениях из документа RFC 2119:

- НЕОБХОДИМО: это слово, а также понятия «ТРЕБУЕТСЯ» или «НУЖНО» означает, что данное определение представляет собой в настоящем отчете безусловное требование.
- НЕ ДОЛЖНО: эта фраза или фраза «НЕ ИМЕЕТ ПРАВА» означает, что данное определение представляет собой в настоящем отчете безусловный запрет.
- СЛЕДУЕТ: это слово или прилагательное «РЕКОМЕНДОВАННЫЙ» означает, что в определенных обстоятельствах могут существовать веские причины игнорировать конкретный пункт рекомендаций, однако следует понять и тщательно взвесить полный спектр последствий, прежде чем избрать иной образ действия.
- НЕ СЛЕДУЕТ: эта фраза или фраза «НЕ СЛЕДУЕТ» означает, что в определенных обстоятельствах могут существовать веские причины считать конкретное поведение приемлемым или даже полезным, однако следует понять и тщательно взвесить ситуацию, прежде чем избрать поведение, которое описано с использованием этого понятия.

III. Пользователи и цели

a. Методология

ЭРГ было рекомендовано в рамках своих усилий по определению служб каталогов регистрации следующего поколения использовать подход с чистого листа, а не пытаться предлагать улучшения существующей системы WHOIS, которая по праву считается неадекватной. В соответствии с директивой Правления ЭРГ начала свой анализ с изучения существующих и потенциальных целей сбора, хранения и предоставления регистрационных данных рДВУ широкому спектру пользователей.

Для выполнения этой задачи члены ЭРГ подготовили обширный набор реальных примеров использования текущей системы WHOIS, анализируя каждый из них с целью выявления (i) пользователей, желающих получить доступ к данным, (ii) их обоснование необходимости такого доступа, (iii) необходимые им элементы данных и (iv) цели, которые достигаются при помощи таких данных. Примеры использования также применялись для выявления заинтересованных сторон, принимающих участие в сборе, хранении и предоставлении регистрационных данных, чтобы ЭРГ смогла понять существующие и потенциальные рабочие процессы и способы, используя которые СКР следующего поколения сможет лучше удовлетворить потребности данных пользователей.

Предполагалось, что эти примеры использования будут не исчерпывающим списком, а скорее репрезентативной выборкой из множества вариантов использования существующей системы WHOIS, иллюстрируя широкий спектр пользователей, их потребностей и рабочих процессов. Перечень рассмотренных ЭРГ примеров использования приведен в Приложении С.

ЭРГ рассмотрела совокупность этих примеров использования и извлеченные из них уроки, чтобы получить консолидированное множество заинтересованных сторон и желательных целей, которые необходимо учитывать в СКР, а также множество потенциальных злоупотреблений, которые система должна постараться предотвратить (см. следующий раздел настоящего отчета). Кроме того, ЭРГ приняла во внимание справочные материалы с результатами предыдущей деятельности, связанной с WHOIS, вклад сообщества и примеры использования для изучения конкретных потребностей в каждой из областей, указанных ниже на Рис. 1.

Рис 1. Анализ потребностей

ЭРГ продолжила свою работу, проанализировав эти цели и потребности пользователей, чтобы получить минимальный набор элементов данных, необходимых для каждой цели, рисков, связанных с предоставлением доступа к этим данным, и последствий этих действий с точки законов о неприкосновенности честной жизни и политики защиты конфиденциальности, а также дополнительные вопросы, изученные в настоящем отчете.

б. Пользователи и цели СКР

На рис. 2 ниже отражена неполная сводная информация о пользователях существующей системы WHOIS, включая тех, кто использует ее в конструктивных целях, и тех, кто использует ее в злонамеренных целях. В соответствии с кругом обязанностей ЭРГ, все эти пользователи были изучены для определения существующих и возможных будущих рабочих процессов и участвующих в них заинтересованных сторон.

Рис 2. Пользователи

В настоящем отчете понятие «инициатор запроса» применяется в общем — ко всем этим пользователям, желающим получить регистрационные данные рДВУ из системы. Как подробнее описано в настоящем отчете, ЭРГ рекомендует отказаться от сегодняшней модели WHOIS, предоставляющей каждому пользователю одинаковый анонимный открытый доступ к (зачастую неточным) регистрационным данным рДВУ. Взамен ЭРГ рекомендует изменить существующую парадигму в пользу сбора, проверки и раскрытия регистрационных данных рДВУ только в разрешенных целях с предоставлением доступа к некоторым элементам данных тем инициаторам запросов, личность которых удостоверена и которые впоследствии будут нести ответственность за их правомерное использование.

ЭРГ проанализировала типичные примеры использования для разработки нижеследующей таблицы, в которой обобщаются виды пользователей, желающих получить доступ к регистрационным данным рДВУ, обоснование необходимости доступа и общие цели, которые достигаются при помощи этих данных. Дополнительные сведения о каждом пользователе, цели и соответствующих данных приведены в разделе III(c), «Разрешенные или запрещенные цели использования» и в Приложении D.

Пользователь	Цель	Примеры вариантов использования	Обоснование необходимости доступа к регистрационным данным
Все владельцы регистраций (например, физические лица, юридические лица, аккредитованные поставщики услуг сохранения конфиденциальности и регистрации через доверенных лиц)	Управление доменным именем	Создание учетной записи регистрации доменного имени	Позволяют всем видам владельцев регистраций регистрировать доменные имена, создав новую учетную запись у регистратора
		Мониторинг изменения данных доменного имени	Обнаружение случайного, несанкционированного изменения регистрационных данных доменного имени или их изменения по причине неосведомленности, как в настоящий момент, так и ранее (при помощи службы WhoWas)
		Управление портфелем доменных имен	Способствует обновлению регистрационных данных всех доменных имен (например, назначенных контактных лиц, адресов) в рамках обслуживания портфеля доменных имен
		Инициирование передачи доменного имени	Позволяет по инициативе владельца регистрации передавать доменное имя другому регистратору
		Удаление доменного имени	Позволяет удалить доменное имя с истекшим сроком регистрации
		Обновление данных DNS для доменного имени	Позволяет по инициативе владельца регистрации изменять данные DNS для доменного имени
		Продление регистрации доменного имени	Позволяет владельцу регистрации продлить срок действия зарегистрированного доменного имени

Пользователь	Цель	Примеры вариантов использования	Обоснование необходимости доступа к регистрационным данным
		Подтверждение контактных данных доменного имени	Способствует первоначальному и непрерывному подтверждению регистрационных данных (например, назначенных контактных лиц, адресов) владельцем регистрации
Защищенные владельцы регистраций (например, заказчики аккредитованных услуг сохранения конфи-денциальности и регистрации через доверенных лиц, с которыми необходимо связаться)	Защита персональных данных	Связь с поставщиком услуг сохранения конфиденциальности/ регистрации через доверенных лиц	Позволяет связаться с аккредитованными поставщиками услуг сохранения конфиденциальности или регистрации через доверенных лиц, которые предоставляют услуги регистрации любому владельцу регистрации, стремящемуся свести к минимуму доступ к своему личному имени или адресу
		Связь с ответственным за утверждение защищенных учетных данных	Позволяет связаться с аккредитованными ответственными за утверждение защищенных учетных данных, которые предоставляют услуги регистрации любым частным лицам или группам, находящимся под угрозой и использующим защищенные учетные данные, переданные доверенной третьей стороной

Пользователь	Цель	Примеры вариантов использования	Обоснование необходимости доступа к регистрационным данным
Технический персонал Интернета (например, администраторы DNS, администраторы почты, веб-администраторы, интернет-провайдеры)	Решение технических проблем	Связь с техническим персоналом доменного имени	Способствует установлению контакта с техническим персоналом (частным лицом, должностным лицом или организацией), способным помочь в решении технических или эксплуатационных проблем с доменными именами (например, ошибок разрешения DNS, проблем с доставкой электронной почты, функциональных проблем на веб-сайте)
Центры сертификации	Сертификация доменного имени	Выдача сертификатов доменных имен	Помогает центру сертификации (ЦС) определить владельца регистрации доменного имени для привязки к сертификату SSL/TLS
Индивидуальные пользователи Интернета (например, потребители)	Индивидуальное использование Интернета	Контакт с реальным миром	Помогает потребителям определять не связанные с Интернетом контактные данные владельца регистрации доменного имени (например, юридический адрес)
		Защита прав потребителей	Предоставляет потребителям простой механизм связи с назначенным владельцем регистрации доменного имени контактным лицом по коммерческим вопросам (например, с отделом обслуживания клиентов розничного интернет-магазина) для быстрого решения проблем без вмешательства правоохранительных органов или служб безопасности

Пользователь	Цель	Примеры вариантов использования	Обоснование необходимости доступа к регистрационным данным
Деловые пользователи Интернета (например, владельцы брендов, брокеры, агенты)	Покупка или продажа доменного имени в деловых целях	Посредническая продажа доменного имени	Позволяет провести комплексную проверку в связи с приобретением доменного имени
		Проверка охраноспособности товарного знака — доменного имени	Позволяет определить владельцев регистраций доменных имен для поддержки проверки охраноспособности товарного знака (анализ рисков) при создании новых брендов
		Приобретение доменного имени	Способствует приобретению ранее зарегистрированного доменного имени, позволяя установить контакт с владельцем регистрации
		Запрос на покупку доменного имени	Позволяет определить доступность доменного имени и текущего владельца регистрации и контактного лица по административным вопросам (если таковой имеется)
		История регистрации доменного имени	Предоставляет данные по истории регистрации доменного имени для определения предыдущих владельцев и дат регистрации с использованием службы WhoWas
		Доменные имена определенного владельца регистраций	Позволяет определить все доменные имена, зарегистрированные конкретным субъектом (обратный запрос) в рамках подтверждения поглощения/разделения активов

Пользователь	Цель	Примеры вариантов использования	Обоснование необходимости доступа к регистрационным данным
Исследователи Интернета	Исследование DNS в научных или обществен-ных интересах	История регистрации доменного имени	Позволяет изучить историю регистрации доменного имени (WhoWas) во время исследования DNS, проводимого в научных или общественных интересах
		Доменные имена конкретного контактного лица	Позволяет определить все домены, зарегистрированные с использованием данного имени, адреса, сервера имен, даты регистрации и т. п. (обратный запрос) во время исследования DNS, проводимого в научных или общественных интересах
		Опрос владельца регистрации доменного имени или назначенного контактного лица	Позволяет проводить опросы владельцев регистраций доменных имен или назначенных контактных лиц
Владельцы интеллектуальной собственности (например, владельцы брендов, товарных знаков, ИС)	Юридические действия	Контакт с пользователем доменного имени	Позволяет установить контакт со стороной, использующей доменное имя, являющееся предметом расследования возможного нарушения прав на товарный знак/бренд или хищения ИС
		Борьба с мошенническим использованием данных владельцев регистраций	Способствует обнаружению мошеннического использования правильных данных (например, адреса) доменных имен, принадлежащих другому владельцу регистрации, путем использования обратного запроса данных о подтверждении личности.

Пользователь	Цель	Примеры вариантов использования	Обоснование необходимости доступа к регистрационным данным
		История регистрации доменного имени	Позволяет изучить историю регистрации доменного имени (WhoWas) во время исследования нарушения прав на ИС
		Доменные имена определенного владельца регистраций	Позволяет определить все домены, зарегистрированные с использованием данного имени или адреса (обратный запрос) во время исследования нарушения прав на ИС
Дознаватели, не являющиеся правоохранительными органами (например, налоговые органы, поставщики ЕПРД, отдел соблюдения договорных обязательств ICANN)	Принуждение к соблюдению нормативных и договорных обязательств	Онлайновое налоговое расследование	Способствует идентификации национальными, региональными или местными налоговыми органами контактных лиц доменных имен, занимающихся онлайн-торговлей
		Разбирательства в рамках ЕПРД (UDRP)	Позволяет поставщикам ЕПРД подтвердить правильность личности ответчика для доменного имени, выполнить проверки соблюдения обязательств, определить требования правового процесса и защитить от киберфлайта (изменения сведений о владельце регистрации с целью уклониться от спора)

Пользователь	Цель	Примеры вариантов использования	Обоснование необходимости доступа к регистрационным данным
		Выполнение договорных обязательств в экосистеме СКР	Позволяет ICANN проводить аудиторские проверки и рассматривать жалобы на несоблюдение контрагентами договорных обязательств (например, касающиеся неточности или недоступности данных, выполнения решения ЕПРД, передачи доменных имен, депонирования и сохранения данных)
Дознаватели из правоохранительных органов/служб безопасности (например, правоохранительные органы, группы реагирования на происшествия)	Расследование уголовных и предотвращение злоупотреблений в DNS	Проведение расследования в отношении неправомочного доменного имени	Позволяет сотрудникам правоохранительных органов/служб безопасности эффективно провести расследование и собрать доказательства в рамках реагирования на обвинения в злонамеренной регистрации доменного имени, в том числе изучить архивные данные
		Расследование преступной деятельности за рамками Интернета	Позволяет сотрудникам правоохранительных органов/служб безопасности эффективно провести расследование и собрать доказательства в рамках реагирования на преступную деятельность за рамками Интернета благодаря предоставлению подробных данных о регистрации и/или поиску доменных имен, зарегистрированных подозреваемым (обратный запрос)
		Услуги оценки репутации доменного имени	Позволяет поставщикам услуг оценки репутации выполнять анализ для составления белых и черных списков доменных имен

Пользователь	Цель	Примеры вариантов использования	Обоснование необходимости доступа к регистрационным данным
		Расследование преступной деятельности в Интернете	Помогает пострадавшим лицам или их адвокатам определить владельца регистрации доменного имени, участвующего в потенциально незаконной деятельности, для обеспечения возможности проведения дальнейшего расследования силами правоохранительных органов и служб безопасности
		Контактные лица по вопросам злоупотреблений для взломанного доменного имени	Помогает устранить последствия взлома доменных имен, содействуя возможности сотрудников правоохранительных органов/служб безопасности установить контакт с владельцем регистрации или назначенным контактным лицом по вопросам злоупотреблений
Широкая общественность (например, блоггеры, СМИ, политические активисты)	Прозрачность DNS	Доступ общественности к регистрационным данным	Определение организации «стоящей за» доменным именем, что часто является желанием широкого спектра пользователей Интернета, не принимающих участия в других более конкретных сценариях использования

Пользователь	Цель	Примеры вариантов использования	Обоснование необходимости доступа к регистрационным данным
Злоумышленники (например, лица, занимающиеся распространением спама, DDoS-атаками, фишингом, хищением персональных данных, перехватом доменов)	Злонамеренная деятельность в Интернете	Перехват доменных имен	Сбор регистрационных данных доменных имен для получения незаконного доступа к учетной записи владельца регистрации и перехвата одного или нескольких доменных имен этого владельца регистрации
		Злонамеренная регистрация доменных имен	Использование существующей/взломанной учетной записи регистрации доменных имен для регистрации новых имен с целью криминальной, мошеннической или зло-намеренной деятельности
		Сбор регистрационных данных для спама/обмана	Сбор регистрационных данных доменных имен для злонамеренного использования спамерами, мошенниками, обманщиками и другими преступниками (злоумышленниками)

Таблица 1. Пользователи и цели СКР

в. Цели, которые следует разрешить или запретить

ЭРГ стремилась определить приоритет целей, перечисленных выше, чтобы сосредоточить внимание на проработке вариантов использования и сузить спектр разрешенных целей. Однако возникли трудности при попытках обосновать необходимость предоставить новую систему только некоторым из пользователей, имеющих доступ к нынешней системе WHOIS, но отказать другим, при условии, что их цели не являются злонамеренными. Этот вывод привел к тому, что ЭРГ рекомендует *некоторым образом* предусмотреть в рамках СКР все указанные разрешенные цели, за исключением известной злонамеренной деятельности в Интернете, которой необходимо активно препятствовать. Таким образом, рекомендованные ЭРГ разрешенные цели обобщены ниже.

Рис 3. Разрешенные цели

Следует отметить, что в рамках каждой цели существует бесконечное число существующих и возможных в будущем вариантов использования. Хотя ЭРГ не пыталась определить все возможные варианты использования, она постаралась изучить их репрезентативную выборку в надежде строго определить виды пользователей и их цели при стремлении получить доступ к регистрационным данным рДВУ. Однако при разработке СКР необходимо предусмотреть возможность охвата новых пользователей и разрешенных целей, которые могут возникнуть с течением времени.

В процессе выполнения ЭРГ анализа вариантов использования, перечисленных в Приложении С, стало понятно, что многим пользователям необходимы одни и те же элементы данных, но для различных целей. Некоторые из таких потребностей широко распространены, например:

- Возможность определить, зарегистрировано ли доменное имя
- Возможность определить текущее состояние домена
- Возможность контакта с каким-либо лицом по вопросам доменного имени

Однако некоторые потребности, несмотря на свою распространенность, не обслуживаются оперативно и последовательно нынешней системой WHOIS. Вот несколько примеров:

- Возможность определить все домены, зарегистрированные конкретным субъектом (что часто называется «обратной WHOIS» (Reverse WHOIS))
- Возможность определить исторические данные о регистрации доменных имен (что часто называется службой WhoWas)

ЭРГ приняла во внимание эти распространенные потребности при разработке рекомендаций по СКР, подробно изложенных в настоящем отчете. Однако поскольку есть вероятность, что с течением времени будут выявлены дополнительные распространенные потребности, любая система следующего поколения должна разрабатываться с достаточной степенью гибкости. Выявленные на настоящий момент ЭРГ разрешенные цели и соответствующие потребности в плане регистрационных данных, контактов и запросов более подробно определены ниже.

Цель	Определение
Управление доменным именем	К задачам, которые находятся в рамках этой цели, относятся создание, управление и контроль над доменным именем, принадлежащим владельцу регистрации (ДИ), в том числе создание ДИ, обновление информации о ДИ, передача ДИ, продление срока регистрации ДИ, удаление ДИ, сопровождение портфеля ДИ и обнаружение мошеннического использования собственных контактных данных владельца регистрации. Это подразумевает, что каждый владелец регистрации для этой цели должен быть авторизованным пользователем СКР и иметь возможность доступа ко всем открытым данным и данным с регулируемым доступом своего ДИ в СКР, в том числе к опубликованным в СКР для этого ДИ сведениям о назначенных контактных лицах.
Защита персональных данных	К задачам, которые находятся в рамках этой цели, относятся идентификация аккредитованного поставщика услуг сохранения конфиденциальности/ регистрации через доверенных лиц, связанного с этим ДИ, и направление такому поставщику сообщений о злоупотреблениях, запросов на раскрытие сведений, или установление иных контактов с этим поставщиком. Для выполнения этих задач пользователю необходима надежная и удобная возможность связи с поставщиком услуг сохранения конфиденциальности/ регистрации через доверенных лиц — например, путем перехода по URL-адресу назначенного поставщиком услуг сохранения конфиденциальности/ регистрации через доверенных лиц ЦКЛ по вопросам злоупотреблений на страницу, где находится описание процедуры раскрытия данных поставщиком или доступная для отправки пользователем форма запроса на раскрытие сведений.

Цель	Определение
Решение технических проблем	К задачам, которые находятся в рамках этой цели, относится работа над решением технических проблем, связанных с использованием доменного имени, включая проблемы доставки электронной почты, ошибки разрешения в DNS, а также функциональные проблемы веб-сайтов. Для выполнения указанных задач у пользователя должна быть возможность связаться с техническим персоналом, отвечающим за решение этих проблем. (Примечание: возможно, целесообразно назначить несколько контактных лиц для решения вопросов разного рода — например, назначить администратора почтовой системы для решения вопросов, связанных с электронной почтой.)
Сертификация доменного имени	К задачам, которые находятся в рамках этой цели, относится выдача Центром сертификации (ЦС) сертификата X.509 субъекту, определяемому доменным именем. Для выполнения этой задачи пользователю необходимо подтвердить, что ДИ зарегистрировано на имя указанного в сертификате субъекта; для этого требуется доступ ко всем открытым и закрытым данным о владельце регистрации.
Индивидуальное использование Интернета	К задачам, которые находятся в рамках этой цели, относятся идентификация организации, использующей доменное имя, для внушения доверия потребителям или установления связи с этой организацией с целью отправки претензий потребителей или подачи жалоб на эту организацию. Для выполнения этих задач пользователю необходимо наименование организации (предпочтительно с подтверждением тождественности) и ее юридический (почтовый) адрес, и может принести пользу возможность перехода по URL-адресу контактного лица на страницу, где находится описание организации и контактные данные службы поддержки клиентов или доступная для отправки пользователем форма запроса в службу поддержки.
Покупка или продажа доменного имени в деловых целях	К задачам, которые находятся в рамках этой цели, относятся отправка запросов на покупку ДИ, приобретение ДИ у другого владельца регистрации и обеспечение возможности проведения юридической экспертизы. Для выполнения этих задач пользователю необходим доступ к адресу организации и адресу электронной почты владельца регистрации, а в некоторых случаях дополнительные закрытые данные — например, для выполнения обратного запроса по имени владельца регистрации или контактного лица, чтобы определить другие доменные имена, к которым они имеют отношение.

Цель	Определение
Исследование DNS в научных или общественных интересах	К задачам, которые находятся в рамках этой цели, относится изучение в научных или общественных интересах доменных имен, сведения о которых опубликованы в СКР, включая общедоступную информацию о владельце регистрации и назначенных им контактных лицах, историю и состояние доменного имени, а также сведения о доменных именах, зарегистрированных конкретным владельцем (обратный запрос). Для выполнения этой задачи пользователю необходим доступ ко всем открытым данным в СКР и в некоторых случаях может потребоваться доступ к закрытым данным для их использования в анонимном, обобщенном виде.
Юридические действия	К задачам, которые находятся в рамках этой цели, относятся расследование возможного мошеннического использования принадлежащего владельцу регистрации имени или адреса другими доменными именами, расследование возможного нарушения прав на торговые марки, установление связи с законным представителем владельца регистрации/лицензии перед юридическим действием и последующее юридическое действие, если проблему не удается разрешить удовлетворительным образом. Для выполнения указанных задач у пользователя должна быть возможность связаться с контактным лицом владельца регистрации/лицензии, которое является его законным представителем, без необходимости действовать через аккредитованного поставщика услуг конфиденциальности/регистрации через доверенных лиц.
Принуждение к соблюдению нормативных и договорных обязательств	К задачам, которые находятся в рамках этой цели, относятся расследование налоговыми органами деятельности компаний, имеющих представительства в Интернете, расследование в рамках ЕПРД (UDRP), расследование соблюдения договорных обязательств и аудиторские проверки депонирования регистрационных данных. Для выполнения этого аккредитованному пользователю необходим доступ к некоторым закрытым контактным данным владельца регистрации и элементам данных ДИ, таким как почтовый адрес и номер телефона, в зависимости от заявленной цели. Например, доступ может потребоваться Всемирной организации по охране интеллектуальной собственности (WIPO) для разрешения вопросов согласно ЕПРД.
Расследование уголовных дел и предотвращение злоупотреблений в DNS	К задачам, которые находятся в рамках этой цели, относятся передача информации о злоупотреблениях лицу, которое может расследовать и устранить данное злоупотребление, или установление связи с организациями, имеющими отношение к доменному имени, во время обычного расследования уголовных дел. Для выполнения этих задач аккредитованному пользователю (например, сотруднику правоохранительных органов, службы быстрого реагирования) необходима надежная возможность быстро связаться с контактным лицом по вопросам злоупотреблений, отвечающим за соответствующее доменное имя — например, путем перехода по URL-адресу на страницу с описанием процедуры сообщения о нарушениях или формой сообщения о происшествии.

Цель	Определение
Прозрачность DNS	К задачам, которые находятся в рамках этой цели, относится отправка запросов на получение регистрационных данных, опубликованных владельцами регистраций, для удовлетворения широкого спектра типовых потребностей широкой общественности в информации. Для выполнения этих задач пользователю необходим удобный доступ к открытым данным (и только к открытым данным), которые могут быть переданы СКР. Владельцев регистрации необходимо информировать о том, что открытые данные о принадлежащих им зарегистрированных доменных именах могут использоваться для этой «универсальной» цели, и данную цель необходимо ограничить открытыми данными (то есть для этой цели НЕ предоставляется доступ к закрытым данным).

Таблица 2. Определения целей

Объем регистрационных данных, которые необходимы для этих целей, дополнительно обобщается в приведенной ниже таблице, где отражены затрагиваемые доменные имена, виды необходимых данных (данные о владельце регистрации, контактные данные, данные о доменном имени), и необходимые дополнительные запросы.

Цель	Объем запроса	Необходимые контакты	Необходимые данные о владельце регистрации	Данные о ДИ	Другие необходимые запросы
Управление доменным именем	Собст-венное ДИ	Все	Открытые + закрытые	Да	Обратный (свои данные) WhoWas (свое ДИ)
Защита персональных данных	ДИ PP*	PP	Открытые	Да	Нет
Решение технических проблем	Любое ДИ	Технические	Открытые	Да	Нет
Сертификация доменного имени	Любое ДИ	Нет	Открытые + закрытые	Да	Нет
Индивидуальное использование Интернета	ДИ LP*	Коммерчески е	Открытые	Нет	Нет
Покупка или продажа доменного имени в деловых целях	Любое ДИ	Административные	Открытые + разрешенные закрытые	Да	Обратный (утвержденные данные) WhoWas (любое ДИ)
Исследование DNS в научных или общественных интересах	Любое ДИ	Все	Открытые + разрешенные закрытые	Да	Обратный (утвержденные данные) WhoWas (любое ДИ)

Цель	Объем запроса	Необходимые контакты	Необходимые данные о владельце регистрации	Данные о ДИ	Другие необходимые запросы
Юридические действия	Любое ДИ	Юридические	Открытые + разрешенные закрытые	Да	Обратный (утвержденные данные) WhoWas (любое ДИ)
Принуждение к соблюдению нормативных и договорных обязательств	Любое ДИ	Юридические	Открытые + закрытые	Да	Обратный (любые данные) WhoWas (любое ДИ)
Расследование уголовных дел и предотвращение злоупотреблений в DNS	Любое ДИ	По вопросам злоупотреб-лений	Открытые + закрытые	Да	Обратный (любые данные) WhoWas (любое ДИ)
Прозрачность DNS	Любое ДИ		Открытые	Да	Нет

Таблица 3. Объем регистрационных данных, необходимых для каждой цели

«Разрешенные закрытые данные» в таблице 3 можно определить на основании Условий предоставления услуг, которые могут быть запрошены аккредитованными пользователями СКР, с учетом установленных политик, охватывающих следующие аспекты:

- Кто имеет право на регулируемый доступ
- Законные причины возникновения необходимости в этих данных
- Ограничения использования этих данных
- Надзор, необходимый для обеспечения надлежащего использования

Эти цели, для которых необходимы «Разрешенные закрытые данные», требуют дополнительного анализа, консультаций с соответствующими сообществами пользователей СКР для определения целесообразных способов выработки, внедрения и обеспечения соблюдения этих политик с сохранением равновесия между потребностями в подотчетности и конфиденциальности. Однако ниже приведены примеры для иллюстрации того, как это могло бы работать:

- **Исследование DNS в научных или общественных интересах** мог бы проводить научный сотрудник признанного университета, занимающийся конкретным исследованием DNS, составивший перечень необходимых закрытых элементов данных и способов их будущего использования, согласившийся публиковать результаты только в обобщенном/анонимном виде при условии надзора со стороны Независимой ревизионной комиссии (НРК). Дав разрешение на выполнение «исследования DNS в общественных интересах», аккредитованному пользователю СКР можно было бы предоставить право доступа к определенным закрытым элементам данных о владельцах регистрации или получения этих элементов данных при помощи обратного запроса.
- **Покупка и продажа ДИ** — это изыскание мог бы проводить деловой пользователь, который занимается коммерческими операциями, требующими юридической экспертизы активов продавца в виде доменных имен. При условии мониторинга и надзора со стороны Аккредитованного органа (определение дано в разделе IV(c), «Аккредитация пользователей СКР»), этот пользователь мог бы заверить не только в том, что он занимается покупкой доменных имен, но и в том, что данные СКР, необходимые для проведения юридической экспертизы продавца «X», и результаты будут использованы только для этой конкретной цели. Дав разрешение на использование DNS для проведения этого вида юридической экспертизы, аккредитованному пользователю СКР можно было бы предоставить право использовать обратные запросы для поиска доменных имен, у которых разрешенные закрытые данные связаны с продавцом «X», как подробнее описано в Приложении E.
- **Юридические действия** — это изыскание мог бы проводить имеющий лицензию юрист, занимающийся расследованием нарушения прав на товарный знак. При условии мониторинга и надзора со стороны Аккредитованного органа (определение дано в разделе IV(c), «Аккредитация пользователей СКР»), этот пользователь мог бы заверить не только в том, что он занимается расследованием возможных юридических действий, но и в том, что запрашиваемые данные СКР предназначены для изучения субъекта «Y», и все полученные сведения будут использоваться только для этой узкой цели. Дав разрешение на использование DNS для проведения этого вида расследования нарушения прав на товарный знак, аккредитованному пользователю СКР можно было бы предоставить право использовать обратные запросы для поиска доменных имен, у которых разрешенные закрытые данные связаны с субъектом «Y», как подробнее описано в Приложении E.

Описание данных, которые необходимы для этих целей, роли разрешенных закрытых данных и средств защиты, которые можно ввести для сохранения подотчетности пользователей и предотвращения злоупотреблений, см. в Приложении E, «Примеры доступа с проверкой и без проверки подлинности».

Это исследование пользователей СКР и разрешенных целей привело ЭРГ к выработке следующих основополагающих принципов, которые дают возможность предоставлять целевой доступ к данным:

№ п/п	Принципы разрешенных целей
1.	ICANN должна опубликовать, в одном месте, дружественную к пользователю политику, описывающую цель и разрешенные варианты использования регистрационных данных, чтобы четко проинформировать владельцев регистраций о причинах сбора этих данных и процедурах их будущей обработки и использования.
2.	Необходимо четко определить разрешенные и не разрешенные способы использования СКР.
3.	СКР должна поддерживать возможность реализации установленных разрешенных целей, в том числе таких вариантов использования, которые предусматривают: • идентификацию владельца регистрации и назначенных для данной цели контактных лиц; • установление связи с назначенными для данной цели контактными лицами; • использование опубликованных реестрами сведений о доменных именах; и • поиск различных компонентов регистрационных данных, которые необходимы для данной цели.
4.	При разработке СКР необходимо предусмотреть возможность охвата новых пользователей и разрешенных целей, которые могут возникнуть с течением времени. • Необходимо определить процедуру подачи заявок. • Заявки необходимо рассматривать с использованием определенных критериев.

	• Заявки, прошедшие проверку, должны оцениваться и утверждаться многосторонней ревизионной комиссией, как это определено в процессе разработки политики. • Утвержденные заявки необходимо включать в состав политики конфиденциальности СКР и периодически внедрять в соответствии с графиком (например, ежеквартально, ежегодно), как это определено в положениях политики. Примечание: см. раздел VI «Элементы данных», где описана процедура добавления новых элементов данных.
5.	ЭРГ рекомендует *некоторым образом* предусмотреть в рамках СКР все указанные разрешенные цели, за исключением известной злонамеренной деятельности в Интернете, которой необходимо активно препятствовать. Цели, которые ЭРГ рекомендует разрешить, обобщены в таблице 1 «Пользователи и цели СКР», а также на рисунке 3 «Разрешенные цели».
6.	Следует осуществлять сбор, проверку и раскрытие регистрационных данных рДВУ только в разрешенных целях с предоставлением доступа к некоторым элементам данных тем инициаторам запросов, личность которых удостоверена и которые впоследствии будут нести ответственность за их правомерное использование.
7.	Каждый владелец регистрации должен иметь возможность доступа ко всем опубликованным в СКР открытым и закрытым данным о своем доменном имени, в том числе к данным о назначенных контактных лицах.

г. Заинтересованные стороны, играющие активную роль в СКР

В следующей таблице представлена репрезентативная совокупность различных заинтересованных сторон, принимающих участие в сборе, хранении, раскрытии и использовании регистрационных данных рДВУ, с которыми сопоставлены соответствующие цели. Некоторые заинтересованные стороны являются поставщиками данных (например, владельцы регистраций), в то время как другие собирают и хранят данные (например, проверяющие, регистраторы, реестры) или раскрывают данные (например, поставщик СКР, аккредитованные поставщики услуг сохранения конфиденциальности и регистрации через доверенных лиц). Однако большинство заинтересованных сторон являются инициаторами запросов данных (например, владельцы брендов и их представители) или лицами, которых идентифицируют, с которыми связываются или на которых раскрытие данных оказывает иное влияние (например, контактные лица по вопросам злоупотреблений при использовании

доменных имен). Эта сводная информация предназначена для того, чтобы проиллюстрировать широту спектра заинтересованных сторон, на которых СКР скорее всего окажет влияние. Однако при осуществлении конкретной транзакции с участием регистрационных данных могут быть дополнительные заинтересованные стороны, не перечисленные здесь.

Заинтересованные стороны	Цели
Агенты и юристы компании-получателя	Покупка или продажа доменного имени в деловых целях
Владелец бренда	Принуждение к соблюдению нормативных и договорных обязательств
Владелец бренда	Покупка или продажа доменного имени в деловых целях
Владелец регистрации	Все цели
Дознаватель	Индивидуальное использование Интернета
Доменный брокер	Покупка или продажа доменного имени в деловых целях
Жертва злоупотребления	Расследование уголовных дел и предотвращение злоупотреблений
Жертва мошенничества	Юридические действия
Интернет-провайдеры	Решение технических проблем Расследование уголовных дел и предотвращение злоупотреблений
Исследователь	Исследование DNS в научных или общественных интересах
Клиент службы сохранения конфиденциальности/регистрации через доверенных лиц	Покупка или продажа доменного имени в деловых целях Управление доменным именем Решение технических проблем Принуждение к соблюдению нормативных и договорных обязательств Защита персональных данных
Компания-получатель	Покупка или продажа доменного имени в деловых целях
Контактное лицо владельца регистрации по правовым вопросам	Юридические действия Принуждение к соблюдению нормативных и договорных обязательств
Контактное лицо по вопросам злоупотреблений для доменного имени	Расследование уголовных дел и предотвращение злоупотреблений
Лицо, занимающееся решением проблемы	Решение технических проблем
Лицо, направившее жалобу	Принуждение к соблюдению нормативных и договорных обязательств
Лицо, сообщившее о проблеме	Решение технических проблем
Лицо/организация, являющееся объектом расследования	Принуждение к соблюдению нормативных и договорных обязательств
Независимая ревизионная комиссия (НРК)	Исследование DNS в научных или общественных интересах
Организация, финансирующая исследования	Исследование DNS в общественных интересах

Ответственный за утверждение защищенных учетных данных	Защита персональных данных
Ответчик в судебном и гражданском процессе	Индивидуальное использование Интернета
Отдел соблюдения договорных обязательств ICANN	Принуждение к соблюдению нормативных и договорных обязательств
Перечисленные контактные лица по административным вопросам	Принуждение к соблюдению нормативных и договорных обязательств Покупка и продажа доменных имен Управление доменным именем Исследование DNS в научных или общественных интересах
Перечисленные контактные лица по вопросам злоупотреблений	Расследование уголовных дел и предотвращение злоупотреблений Управление доменным именем Исследование DNS в научных или общественных интересах
Перечисленные контактные лица по коммерческим вопросам	Индивидуальное использование Интернета Управление доменным именем Исследование DNS в научных или общественных интересах
Перечисленные контактные лица по правовым вопросам	Юридические действия Принуждение к соблюдению нормативных и договорных обязательств Исследование DNS в научных или общественных интересах
Перечисленные контактные лица по техническим вопросам	Решение технических проблем Управление доменным именем Исследование DNS в научных или общественных интересах
Перечисленные контактные лица поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц	Защита персональных данных Управление доменным именем Исследование DNS в научных или общественных интересах
Персонал государственных органов	Принуждение к соблюдению нормативных и договорных обязательств
Персонал правоохранительных органов	Расследование уголовных дел и предотвращение злоупотреблений Юридические действия
Покупатель домена	Покупка или продажа доменного имени в деловых целях
Покупка потребителями товаров на веб-сайтах	Индивидуальное использование Интернета
Получатель защищенных учетных данных	Защита персональных данных
Пользователи Интернета, посещающие веб-сайты	Индивидуальное использование Интернета
Поставщик онлайн-услуг	Решение технических проблем
Поставщик СКР	Все цели
Поставщик услуг веб-хостинга	Решение технических проблем
Поставщик услуг ЕПРД	Принуждение к соблюдению нормативных и договорных обязательств

Поставщик услуг сохранения конфиденциальности/регистрации через доверенных лиц	Расследование уголовных дел и предотвращение злоупотреблений Покупка или продажа доменного имени в деловых целях Управление доменным именем Исследование DNS в общественных интересах Решение технических проблем Юридические действия Защита персональных данных Принуждение к соблюдению нормативных и договорных обязательств Решение технических проблем
Поставщик услуг управления брендами	Управление доменным именем
Поставщики служб безопасности	Расследование уголовных дел и предотвращение злоупотреблений
Представители владельца регистрации	Управление доменным именем
Представитель жертвы мошенничества	Юридические действия
Проверяющий	Все цели
Регистратор	Покупка или продажа доменного имени в деловых целях Управление доменным именем Исследование DNS в общественных интересах Индивидуальное использование Интернета Юридические действия Защита персональных данных Принуждение к соблюдению нормативных и договорных обязательств Решение технических проблем Расследование уголовных дел и предотвращение злоупотреблений
Реестр	Все цели
Реселлер	Управление ДИ Расследование уголовных дел и предотвращение злоупотреблений
Служба подтверждения адреса	Управление доменным именем
Третьи стороны, стремящиеся установить контакт	Юридические действия Защита персональных данных
Центр сертификации	Сертификация доменного имени
Члены комиссии ЕПРД	Принуждение к соблюдению нормативных и договорных обязательств

Таблица 4. Репрезентативная совокупность заинтересованных сторон

д. Принципы использования целевых контактных лиц

Существование и использование доменных имен Интернета в общедоступных зонах приводит к потенциальным внешним воздействиям на третьих лиц по всему миру. От злоупотреблений и технических проблем до нарушения прав и крупных и мелких проблем с доменными именами есть бесчисленное множество причин возникновения у третьей стороны в каком-то уголке мира законной потребности

связаться с человеком или организацией, имеющими отношение к конкретному доменному имени.

В то же время, у владельцев регистраций доменных имен может возникнуть желание и право (в зависимости от местной юрисдикции) на неприкосновенность частной жизни. Возможно, они не пожелают делать общеизвестными свои контактные данные. Кроме того, зачастую владельцы регистрации не являются лучшими лицами или организациями для решения проблем, которые может поднять третья сторона, — например, проблем, связанных с конфигурацией DNS для доменного имени или реагированием на спор по товарным знакам. Поэтому предоставление информации только о владельцах регистрации, скорее всего, не удовлетворит потребности третьих лиц, которые стремятся разрешить проблемы, возникшие в связи с доменным именем.

Многообразный характер потенциальных проблем потребует различного реагирования — как в плане содержания, так и в плане сроков — на ситуации, которые часто по логике вещей решаются разными людьми и/или организациями, связанными с конкретным доменом. Однако для любого доменного имени, как минимум, должна быть опубликована общедоступная и достоверная информация об одном или нескольких доступных контактных лицах, способных ответить на внешние вопросы и создать точку привязки для разрешенных целей внешних участников, которых затрагивает существование или деятельность доменного имени.

Своевременность ответа может быть желательной целью при разработке политики для конкретных видов контактных лиц. Однако эта цель должна быть сбалансирована с бременем, которое требования в плане реагирования могут наложить на субъектов, выполняющих эти роли. Стремление обойти систему, ненадлежащие запросы или намеренное создание перегрузки для контактных лиц не должно приводить к каким-либо штрафным санкциям для этих контактных лиц. Желательно, чтобы у инициаторов запросов была процедура передачи на более высокий уровень проблемы, возникающей из-за невозможности установить для определенных целей связь с не отвечающим контактным лицом (например, при устранении злоупотреблений, при реагировании на документы, представленные согласно ЕПРД). Отсутствие ответа в рамках такого процесса может привести к приостановке деятельности и/или удалению этого контактного лица и, возможно, затрагиваемых доменных имен в соответствии с официальной процедурой. Однако конкретные цели политики обеспечения своевременности реагирования выходят за рамки настоящего отчета.

№ п/п	Принципы использования целевых контактных лиц
8.	Для каждого зарегистрированного доменного имени необходимо предоставлять сведения по крайней мере об одном целевом контактном лице (ЦКЛ), что сделает общеизвестной совокупность всех обязательных элементов данных для всех обязательных ЦКЛ. Чтобы отвечать потребностям каждой официально разрешенной цели, сведения об этом ЦКЛ должны быть синтаксически точными и оперативно доступными.
9.	Во время регистрации доменного имени идентификатор контактного лица владельца регистрации[6] необходимо использовать по умолчанию как идентификатор ЦКЛ для каждой цели. Владельца регистрации необходимо проинформировать обо всех разрешенных целях и дать ему возможность опубликовать идентификаторы остальных ЦКЛ для каждой цели, в том числе заменить идентификатор контактного лица владельца регистрации для любой или всех целей.
10.	Целевое контактное лицо не обязательно должно быть владельцем регистрации, и доступ к сведениям о владельце регистрации может быть крайне ограничен в соответствии с остальными политиками. Следует обратить внимание, что ЦКЛ не обязательно означает физическое лицо, а скорее представляет собой назначаемую для различных целей точку контакта.
11.	Нельзя активировать (вводить в глобальную DNS) доменное имя до тех пор, пока для каждой применимой цели не будет указан действительный идентификатор ЦКЛ. Если ЦКЛ больше не может выполнять назначенную ему цель, должна выполняться процедура, позволяющая владельцу регистрации указать новое действующее контактное лицо, которая предусматривает целесообразные уведомления и достаточный для обновления идентификатора ЦКЛ срок. Согласно принципу № 9 выше, идентификатор контактного лица владельца регистрации необходимо использовать по умолчанию как идентификатор ЦКЛ для каждой цели. Непредставление в установленный срок сведений о действующем идентификаторе ЦКЛ может привести к временному исключению и/или удалению доменного имени в соответствии с официальной процедурой. (См. раздел V, где изложены требования к подтверждению.)

[6] Идентификаторы контактных лиц — это идентификаторы, связанные с блоками контактных данных для обеспечения возможности извлечения и обновления сведений, которые введены в разделе IV(a) «Элементы данных» и определены в разделе V(d) «Организационная структура идентификаторов контактных лиц».

№ п/п	Принципы использования целевых контактных лиц
12.	По желанию, идентификатор ЦКЛ может быть указан для каждой разрешенной цели с применением различных установленных требований к сбору и опубликованию необходимых элементов данных для каждого типа ЦКЛ, позволяющих добиться соответствующих разрешенных целей.
13.	Необходимо разработать процедуру и политики, позволяющие назначенным владельцем регистрации контактным лицам соглашаться или не соглашаться на опубликование своих идентификаторов контактных лиц в качестве идентификаторов ЦКЛ для доменных имен, чтобы реализовать право физических и юридических лиц на подтверждение или отклонение обязанности выполнять определенные функции для конкретных зарегистрированных доменных имен.
14.	Любая система предоставления сведений о «целевых контактных лицах» должна быть гибкой и должна давать возможность создания и опубликования в СКР новых целей и типов контактных лиц. (Дополнительные сведения о добавлении новых целей см. в разделе III(c).)

e. Функции и обязанности целевых контактных лиц

Как представлено в обобщенном виде на рисунке 4 и подробно изложено в таблице 1, ЭРГ проанализировала типичные примеры использования, чтобы выявить виды пользователей, желающих иметь доступ к регистрационным данным рДВУ, и разрешенные цели, для которых в настоящее время используются эти данные. Чтобы обеспечить целевой доступ к регистрационным данным все разрешенные цели были сопоставлены с ЦКЛ. Например:

- Контактное лицо по «правовым» вопросам можно назначить для разрешения спросов по товарным знакам или урегулирования других правопритязаний, имеющих отношение к доменному имени. Чтобы обеспечить возможность установления связи для указанных целей, у этого ЦКЛ должен быть только физический адрес, позволяющий получать официальные уведомления, действующий адрес электронной почты для получения запросов и рабочий номер телефона или факса для ответа на вопросы.
- Контактное лицо по вопросам «злоупотреблений» может быть назначено для рассмотрения запросов, касающихся неправомерных действий, источником которых является доменное имя, проявляющихся в виде трафика или другой критичной по срокам злонамеренной деятельности в Интернете. Чтобы обеспечить возможность установления связи для указанных целей, у этого ЦКЛ должен быть адрес электронной почты для получения запросов и отправки

ответов на них, а также действующий номер телефона для получения запросов. Для этого ЦКЛ также можно указать адреса в социальных сетях и сервисах передачи мгновенных сообщений, способствующие взаимодействию в режиме реального времени, физический адрес или номер факса для получения вопросов, а также URL-адрес, который упрощает отправку сообщений о злоупотреблениях.

Также рекомендуется назначать ЦКЛ для решения административных и технических вопросов, для связи с поставщиком услуг сохранения конфиденциальности/ регистрации через доверенных лиц и коммерческих контактов. Полный перечень типов и обязанностей ЦКЛ приведен в таблице 5; см. также раздел IV, «Принцип сбора данных № 20», где указаны элементы данных, необходимые для каждого типа ЦКЛ.

Как показано на следующем рисунке, ЭРГ рекомендует использовать собственный идентификатор владельца регистрации, если для данного доменного имени не указаны более специализированные ЦКЛ. Например, если для данного доменного имени не указано контактное лицо по правовым вопросам, владельца регистрации следует проинформировать о возможном желании других сторон связаться с ним для этой разрешенной цели и дать ему возможность назначить ЦКЛ для получения подобных запросов относительно этого доменного имени.

Если владелец регистрации примет решение не назначать ЦКЛ, такие запросы будут направляться владельцу регистрации с использованием необходимых для этой цели данных, связанных с идентификатором контактного лица владельца регистрации. Если владелец регистрации предпочитает не делать общедоступными эти элементы данных, доменное имя может быть зарегистрировано с использованием услуг сохранения конфиденциальности/регистрации через доверенных лиц. Принципы использования элементов данных и ЦКЛ более подробно рассматриваются в разделе IV.

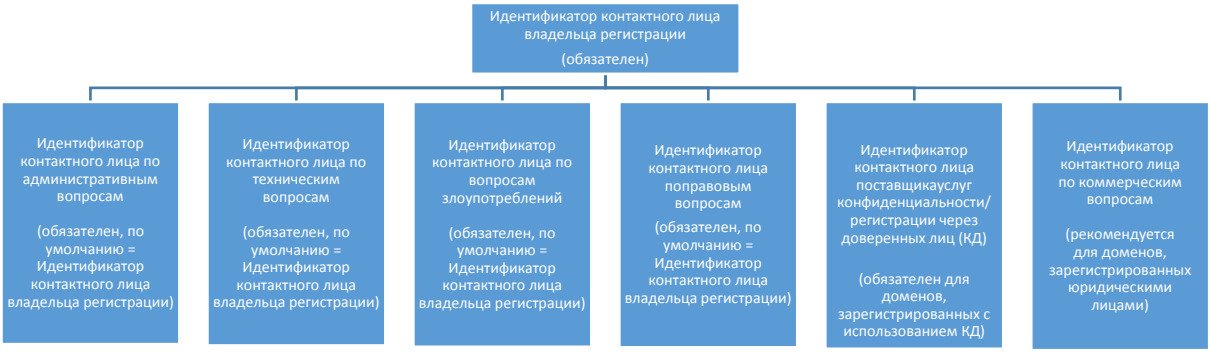


Рис. 4. Типы контактных лиц в СКР

Все цели и контактные лица должны быть официально закреплены органами, формирующими политику, в составе установленной процедуры добавления, изменения или удаления целей.

Этот подход к ЦКЛ сохраняет простоту для владельцев регистраций с базовыми потребностями в контактах и предлагает возможность дополнительной детализации для владельцев регистраций с более широкими потребностями в контактах. Чтобы проиллюстрировать данную концепцию, ниже приведены три различных вымышленных, но типичных примера:

1. Владелец регистрации может прямо назначить идентификатор контактного лица владельца регистрации как единственную току контакта для своего доменного имени. В этом случае в ответ на запросы к СКР для всех разрешенных целей будут возвращаться необходимые для каждой цели авторизованные открытые или защищенные элементы данных, связанные с идентификатором контактного лица владельца регистрации.

Пример регистрационной записи ДИ:

```
Registrant  Contact  ID  =  <reg>
Tech    Contact    ID    =    <reg>
Admin    Contact    ID    =    <reg>
Abuse    Contact    ID    =    <reg>
Legal    Contact    ID    =    <reg>
```

2. Владелец регистрации, использующий аккредитованную услугу **сохранения конфиденциальности** (определение дано в разделе VII), может назначить несколько уникальных идентификаторов контактных лиц для своего доменного имени, включая идентификатор контактного лица поставщика услуг конфиденциальности/ регистрации через доверенных лиц (то есть поставщика услуг сохранения конфиденциальности), идентификатор контактного лица по техническим вопросам (например, поставщика услуг хостинга или интернет-провайдера), и предоставленные поставщиком идентификаторы контактных лиц по административным вопросам, по вопросам злоупотреблений и по правовым вопросам. В этом примере назначенное контактное лицо по техническим вопросам отвечает за решение всех технических проблем, связанных с доменных именем, а контактное лицо поставщика услуг конфиденциальности/ регистрации через доверенных лиц отвечает за все связанные с этим доменным именем услуги сохранения конфиденциальности (в том числе за пересылку владельцу регистрации сообщений, поступивших контактным лицам по административным и правовым вопросам, а также по вопросам злоупотреблений).

Пример регистрационной записи ДИ:

```
Registrant  Contact  ID  =  <reg>
PP    Contact    ID    =    <pp>
Tech    Contact    ID    =    <isp>
Admin    Contact    ID    =    <reg@pp>
Abuse    Contact    ID    =    <reg@pp>
Legal    Contact    ID    =    <reg@pp>
```

3. Владелец регистрации, который идентифицировал себя как юридическое лицо, может представить для данного доменного имени много уникальных идентификаторов контактных лиц, в том числе идентификаторы ЦКЛ по правовым и коммерческим вопросам, а также по вопросам злоупотреблений, связанные с этим конкретным доменным именем. В этом примере в ответ на запросы к СКР для каждой из указанных целей будут возвращены элементы данных, связанные с соответствующим идентификатором конкретного ЦКЛ, что способствует установлению связи с физическим или юридическим лицом, взявшим на себя ответственность за выполнение соответствующей функции. Такой сценарий со временем может получить большее распространение, по мере того как крупные организации начнут пользоваться этой детализацией для улучшения возможности установления связи и сокращения непонимания и переадресации.

Пример регистрационной записи ДИ:

```
Registrant Contact ID = <reg>
Tech Contact ID = <isp>
Admin Contact ID = <admin@reg>
Abuse Contact ID = <abuse@reg>
Legal Contact ID = <legal@reg>
Business Contact ID = <cs@reg>
```

Эти примеры проиллюстрированы графически на приведенном ниже рисунке:

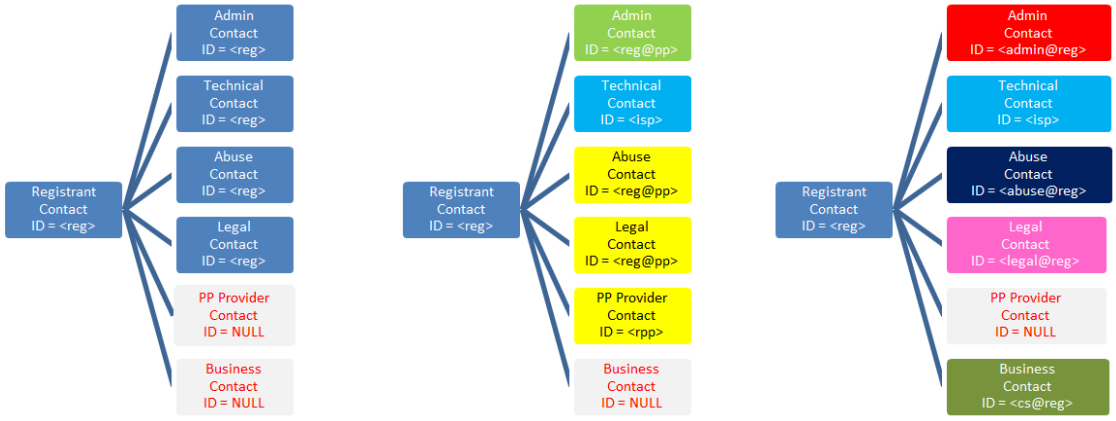


Рис. 5. Примеры регистрации ДИ с использованием целевых контактных лиц

См. список рекомендованных ЦКЛ в разделе IV и полный перечень связанных с каждой разрешенной целью элементов данных и соответствующих ЦКЛ в Приложении D.

В круг обязанностей ЦКЛ входит получение запросов, относящихся к этому доменному имени, оценка этих запросов и подтверждение получения и/или

уведомление владельца регистрации/лицензии, в зависимости от соглашения между владельцем регистрации и ЦКЛ.

Потенциальные обязанности каждого ЦКЛ можно обобщить следующим образом:

Тип ЦКЛ	Потенциальные обязанности
Административные	Обработка запросов, связанных с приобретением и продажей доменных имен, таких как запросы на покупку и передачу доменных имен.
Правовые	Обработка касающихся этого доменного имени запросов, которые поступают от налоговых органов, лиц, проводящих расследование согласно ЕПРД, лиц, проводящих расследование соблюдения договорных обязательств, и законных представителей.
Технические	Обработка касающихся этого доменного имени запросов, которые связаны с перерывами в работе веб-сайта, проблемами DNS, проблемами доставки почты и т. д.
Злоупотребления	Обработка сообщений о касающихся этого доменного имени злоупотреблениях в DNS, включая фишинг, спам и другую вредоносную деятельность в Интернете.
Конфиденциальность и доверенные лица	Обработка запросов на передачу/раскрытие сведений, прием от имени владельца регистрации/лицензии претензий в связи со злоупотреблениями, касающимися доменного имени, выполнение требований в рамках расследования криминальной деятельности правоохранительными органами.
Коммерческие	Обработка запросов потребителей на предоставление коммерческой информации и информации для связи с компанией для получения дополнительных сведений или устранения претензий клиентов.

Таблица 5. Потенциальные обязанности каждого целевого контактного лица

Для будущего рассмотрения: Для каждого типа ЦКЛ может быть указано несколько ЦКЛ, что позволяет установить прямой контакт с конкретными лицами, имеющими критически важные обязанности. Например для широкого присутствия в Интернете желательно разделить технические вопросы между администратором почтовой системы, оператором DNS, веб-мастером и т. д. Обязанности, выполняемые такими специализированными контактными лицами, можно было бы указывать в поле, публикуемом в составе открытых данных с целью идентификации конкретной цели, для которой это ЦКЛ назначено владельцем регистрации. Такая сложная схема, возможно, нецелесообразна в настоящее время, но не следует исключать возможность ее использования в будущем.

ж. Разрешение на использование контактных лиц в СКР

Как описано выше, при регистрации доменного имени необходимо назначить по крайней мере минимально необходимое количество ЦКЛ. Всем таким контактным лицам каждого зарегистрированного доменного имени должно быть известно о назначенных им функциях и они должны согласиться на их выполнение.
Связанные с данной концепцией принципы подробнее рассмотрены ниже.

№ п/п	Принципы выдачи разрешения на использование контактных лиц в СКР
15.	Во избежание задержек при регистрации или обновлении доменного имени, процедура получения одобрения на использование каждого ЦКЛ должна быть масштабируемой и выполняемой в режиме реального времени или близком к реальному времени.
16.	Политики и процедуры должны предотвращать несанкционированное использование ЦКЛ.
17.	Как у ЦКЛ, так и у владельца регистрации должна быть возможность аннулирования этого одобрения в более позднее время. (Подробные сведения см. в разделе V, «Подтверждение»)
18.	У владельцев регистраций должна быть удобная возможность назначения себя в качестве ЦКЛ для своих доменных имен без необходимости получения одобрения у внешней/третьей стороны.

Например, владелец регистрации отправляет идентификатор ЦКЛ и метку для однократного использования, которые могут мгновенно и автоматически подтверждаться проверяющим, который отвечает за этот идентификатор контактного лица. В качестве альтернативы, в процессе получения одобрения контактного лица можно использовать систему подтверждения по электронной почте или SMS.

IV. Повышение подотчетности

Для рекомендованной СКР используется подход с чистого листа, который предусматривает отказ от универсальной модели WHOIS в пользу целенаправленного доступа к проверенным данным с надеждой на улучшение конфиденциальности, точности и ответственности.

ЭРГ считает, что эта парадигма регулируемого доступа способна повысить ответственность всех сторон, участвующих в раскрытии и использовании данных о регистрации доменных имен рДВУ. Во-первых, СКР осуществляла бы учет всего доступа к регистрационным данным рДВУ, в том числе доступа без проверки подлинности к открытым элементам данных и ограничений доступа для предотвращения массового сбора данных. Кроме того, регулируемый доступ к более конфиденциальным элементам данных был бы доступен только тем инициаторам запросов, которые подали заявку и получили учетные данные, позволяющие выполнить аутентификацию запросов к СКР. И наконец, СКР обеспечивала бы аудит доступа как к открытым, так и к защищенным данным с целью минимизации злоупотреблений и применения штрафов и других санкций за неправомерное использование. Для разных целей могли бы применяться различные условия и положения. В случае нарушения инициатором запросов условий и положений могли бы применяться штрафные санкции.

Многие члены сообщества ICANN выразили опасения в связи с отказом от абсолютно анонимной открытой WHOIS в пользу рекомендованной ЭРГ парадигмы регулируемого доступа. Некоторые предложили сохранить открытость всех регистрационных данных для полностью анонимных инициаторов запросов, в то время как другие предложили сделать общедоступной малую часть данных или закрыть доступ ко всем данным. Некоторые поддержали концепцию аккредитации пользователей, запрашивающих доступ для разрешенных целей, но хотели получить дополнительные сведения о доступных элементах данных, процедурах аккредитации и о том, как можно было бы сформировать и доработать с течением времени политики, относящиеся к разрешенным целям. Хотя нет простого ответа, позволяющего обеспечить соответствие всем этим многообразным мнениям, в настоящем разделе подробно изложены рекомендации ЭРГ в этих областях.

a. Принципы для элементов данных

ЭРГ рекомендует следующие принципы систематизации элементов данных.

№ п/п	Принципы для элементов данных
19.	СКР должна предусматривать возможность целенаправленного раскрытия элементов данных. (Список разрешенных целей и соответствующих целевых контактных лиц (ЦКЛ) см. в разделе III.)
20.	Не все собранные данные должны быть общедоступными; раскрытие должно зависеть от инициатора запроса и цели.
21.	Необходимо предоставить публичный доступ к установленному минимальному набору данных, в том числе к сведениям о ЦКЛ, которые опубликованы специально для содействия установлению связи для этой цели.
22.	Элементы данных, которые будут признаны более конфиденциальными (после проведения оценки рисков и последствий), должны быть защищены с предоставлением только авторизованного доступа на основе: • Идентификации разрешенной цели • Раскрытие личности инициатора запроса/цели • Проверка/обеспечение выполнения требования о недопустимости злоупотреблений авторизованным доступом
23.	Необходимо раскрывать (то есть возвращать в ответ на запросы или поиск посредством обратных запросов и запросов WhoWas) только те элементы данных, которые соответствуют заявленной цели.
24.	Необходимо осуществлять сбор только тех элементов данных, которые необходимы для реализации хотя бы одной из разрешенных целей.
25.	Каждый элемент данных должен быть связан с совокупностью разрешенных целей. • В настоящем отчете определено первоначальное множество допустимых вариантов использования, разрешенных целей и необходимых элементов данных (см. раздел III и Приложение D). • Каждая разрешенная цель должна быть связана с четко сформулированными политиками получения доступа и использования элементов данных. • Как указано в разделе III, необходимо определить процедуру непрерывного пересмотра для рассмотрения предлагаемых новых целей и периодического обновления разрешенных целей, позволяющего отразить одобренные дополнения и сопоставить их с существующими элементами данных.

№ п/п	Принципы для элементов данных
	• Необходимо разработать процедуру определения политики для рассмотрения предлагаемых новых элементов данных, обновления получивших определение элементов данных, по мере необходимости, и их сопоставления с существующими разрешенными целями.
26.	Минимальный список элементов данных, подлежащих сбору, хранению и раскрытию, должен создаваться на основе известных примеров использования (отраженных в настоящем документе) и оценки рисков (которую необходимо выполнить до внедрения СКР).
27.	Все реестры и проверяющие обязаны хранить полную совокупность собранных ими/переданных в СКР элементов данных. (См. также раздел VII «Возможные модели СКР».)

Этап 1. Сбор данных

Данные необходимо собрать, прежде чем можно будет осуществлять их выборочное раскрытие для разрешенных целей. Сбор во время регистрации рекомендуется выполнять в соответствии со следующими принципами:

№ п/п	Принципы сбора данных
28.	В подтверждение соблюдения главных правовых принципов, приведенных в разделе VI, регистраторы и проверяющие должны предоставить владельцам регистраций и целевым контактным лицам доменных имен возможность на этапе сбора данных дать согласие на использование своих данных для заранее указанных разрешенных целей в соответствии с действующими в их юрисдикции законами о защите данных. При выработке политики этот принцип следует рассматривать в более широком контексте главных правовых принципов.[7]
29.	Для удовлетворения основных потребностей в управлении доменами реестры и регистраторы обязаны собирать, а владельцы регистраций — предоставлять при регистрации доменного имени следующие элементы данных: а) Доменное имя б) Серверы DNS в) Имя владельца регистрации

[7] Эта формулировка была поддержана почти единогласно, один член ЭРГ возражал.

№ п/п	Принципы сбора данных
	г) Тип владельца регистрации Указывает тип субъекта, определяемого именем владельца регистрации, и при предъявлении требований к регистрационным данным подлежит использованию следующим образом: **Не указан** — применяется по умолчанию, если не выбран ни один из перечисленных ниже вариантов, и должен обрабатываться в СКР аналогично физическому лицу. **Поставщик услуг конфиденциальности/регистрации через доверенных лиц** — необходимо выбирать для доменных имен, зарегистрированных с помощью аккредитованного поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц. При выборе этого варианта также должен быть указан идентификатор контактного лица аккредитованного поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц, чтобы обеспечить возможность отправки в адрес ЦКЛ КД запросов на передачу и раскрытие данных. **Юридическое лицо** — можно выбирать для доменных имен, зарегистрированных на имя субъектов, которые НЕ являются физическими лицами И НЕ являются аккредитованными поставщиками услуг регистрации через доверенных лиц. При выборе этого варианта также должен быть указан идентификатор назначенного ЦКЛ по коммерческим вопросам, чтобы содействовать отправке потребителями запросов и жалоб (см. примечание под данной таблицей). **Физическое лицо** — можно выбирать для доменных имен, зарегистрированных на имя физических лиц. При выборе этого варианта не должно быть указано ни ЦКЛ поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц, ни ЦКЛ по коммерческим вопросам, а имя и адрес владельца регистрации должны обрабатываться как персональные данные в соответствии с законами о защите данных, действующими в юрисдикции субъекта данных. д) Идентификатор контактного лица владельца регистрации Уникальный идентификатор, присваиваемый каждому контактному лицу владельца регистрации [имя+адрес] во время подтверждения (более подробное определение идентификатора контактного лица, а также процесса его создания проверяющим и использования для регистрации ДИ см. в разделе V Improving Data Quality).

№ п/п	Принципы сбора данных
	е) Почтовый адрес владельца регистрации Содержит следующие элементы данных: улица, город, штат/регион, почтовый индекс, страна (сообразно обстоятельствам). ж) Адрес электронной почты владельца регистрации з) Телефон владельца регистрации Содержит следующие элементы данных: номер, добавочный номер (если применимо).
30.	а) В целях одновременного улучшения защиты конфиденциальности владельцев регистраций и возможности установления контактов с ними, регистраторы обязаны собирать, а владельцы регистраций — предоставлять данные о Целевых контактных лицах (ЦКЛ) для каждого зарегистрированного доменного имени. б) По желанию, владельцы регистраций имеют право указывать ЦКЛ поставщиков услуг сохранения конфиденциальности/регистрации через доверенных лиц или правомочных ЦКЛ третьей стороны для конкретных разрешенных целей (см. раздел III). в) Чтобы удовлетворить потребности в установлении контактов, возникающие в связи с каждой разрешенной целью, созданные через проверяющего и впоследствии связанные с доменным именем ЦКЛ должны отвечать следующим минимально необходимым требованиям к элементам данных: Контактное лицо по техническим вопросам: адрес электронной почты Контактное лицо по административным вопросам: организация, адрес электронной почты Контактное лицо по правовым вопросам: организация, адрес электронной почты, телефон, почтовый адрес Контактное лицо по вопросам злоупотреблений: адрес электронной почты, номер телефона Контактное лицо по коммерческим вопросам[8]: организация, почтовый адрес Контактное лицо поставщика услуг сохранения конфиденциальности/ регистрации через доверенных лиц[9]: организация, адрес электронной почты, URL-адрес контактного лица, URL-адрес по вопросам злоупотреблений

[8] Контактное лицо является обязательным только в том случае, если тип владельца регистрации = юридическое лицо

[9] Контактное лицо является обязательным только в том случае, если тип владельца регистрации = поставщик услуг сохранения конфиденциальности/регистрации через доверенных лиц

№ п/п	Принципы сбора данных
	г) Если владелец регистрации не назначает ЦКЛ для каждой обязательной разрешенной цели, для этих ЦКЛ по умолчанию должен использоваться собственный идентификатор контактного лица владельца регистрации. (Следует обратить внимание, что владелец регистрации может избежать этого, воспользовавшись услугой сохранения конфиденциальности/ регистрации через доверенных лиц или назначив ЦКЛ.) Когда в качестве идентификатора ЦКЛ используется идентификатор контактного лица владельца регистрации, требования в отношении сбора и раскрытия данных о владельце регистрации могут быть увеличены для удовлетворения указанных выше потребностей в наличии обязательных элементов данных ЦКЛ.
31.	Чтобы избежать получения избыточного количества данных, сбор всех остальных предоставляемых владельцем регистрации данных, не перечисленных в принципах № 29 и 30 выше и используемых по крайней мере для *одной* разрешенной цели, должен осуществляться по желанию владельца регистрации. Проверяющие, реестры и регистраторы обязаны предусмотреть возможность получения и хранения этих данных по желанию владельца регистрации.
32.	Для обеспечения максимальной стабильности Интернета реестры и регистраторы должны предоставлять в СКР следующие обязательные элементы данных: а) Состояние регистрации б) Состояние на стороне клиента (устанавливает регистратор) в) Состояние на стороне сервера (устанавливает реестр) г) Регистратор д) Юрисдикция регистратора е) Юрисдикция реестра ж) Язык соглашения о регистрации з) Дата создания и) Дата истечения срока действия регистрации к) Дата обновления л) URL-адрес регистратора м) Идентификатор IANA регистратора н) Номер телефона контактного лица регистратора по вопросам злоупотреблений о) Адрес электронной почты контактного лица регистратора по вопросам злоупотреблений п) URL-адрес сайта Internic для отправки жалоб

№ п/п	Принципы сбора данных
33.	Что касается элементов данных, характерных для конкретного ДВУ, реестр ДВУ должен сформировать и опубликовать политику сбора данных (соответствующую этим главным принципам) и нести ответственность за любую проверку этих специфичных для ДВУ элементов данных.
34.	Проверяющие, реестры и регистраторы имеют право для внутреннего использования собирать, хранить и раскрывать дополнительные элементы данных, которые никогда не передаются в СКР.[10]

Примечание: После серьезного обсуждения ЭРГ не рекомендовала добавить в состав элементов данных **Назначение доменного имени**. Вместо этого ЭРГ рекомендовала принципы, позволяющие достичь соответствующих целей, а также рекомендовала конкретное **ЦКЛ по коммерческим вопросам** для опубликования владельцами регистраций, которые идентифицируют себя в качестве **юридических лиц**, занимающихся коммерческой деятельностью. Это может привести к опубликованию многими коммерческими пользователями Интернета более единообразных элементов данных для повышения доверия потребителей, хотя при этом признается, что в конечном итоге владельцы регистраций сами выбирают эту классификационную группу, и было бы практически невозможно в мировом масштабе принудить к строгому соблюдению требования указывать назначение доменного имени = коммерческое или некоммерческое.

Этап 2. Раскрытие данных

После сбора данных можно осуществлять их выборочное раскрытие для разрешенных целей. При получении запросов данные рекомендуется раскрывать в соответствии со следующими принципами:

[10] Например, к таким данным относится IP-адрес клиента в момент регистрации, ссылка на запрос о создании ключа передачи EPP для доменного имени и платежные данные, связанные с учетной записью клиента. Предназначенные для внутреннего использования данные не стандартизированы в СКР, и вместо этого определяются в частном порядке реестрами и регистраторами.

№ п/п	Принципы раскрытия данных
35.	Для максимальной защиты конфиденциальности владельцев регистраций, передаваемые ими данные по умолчанию должны быть защищены, кроме тех случаев, когда есть насущная необходимость открытого доступа к данным, которая превышает возникающий в результате опубликования риск. • По своему желанию, владельцы регистрации могут на основе осознанного согласия сделать общедоступными любые свои защищенные данные.
36.	Для обеспечения максимальной стабильности Интернета, все регистрационные данные, предоставленные реестром или регистратором, всегда должны быть общедоступными, кроме тех случаев, когда это приводит к неприемлемому риску. • По своему желанию, владельцы регистрации могут сделать любые общедоступные данные реестра/регистратора закрытыми, кроме указанных ниже случаев, когда данные необходимы для основных операций управления доменом.
37.	Для максимального повышения доступности, все ЦКЛ должны быть общедоступными по умолчанию. • По своему желанию, владельцы контактных данных[11] могут сделать любые элементы данных ЦКЛ закрытыми, за исключением тех, которые необходимы для соответствующей цели (подробнее рассматривается в таблице 5).
38.	Для удовлетворения основных потребностей в управлении доменами необходимо включить в состав минимального множества общедоступных данных следующие полученные от владельца регистрации данные, которые обязательны для сбора и создают небольшой риск в случае раскрытия: а) Доменное имя б) Серверы DNS

[11] В соответствии с разделом III(g), «Разрешение на использование контактных лиц в СКР», назначенные ЦКЛ должны давать разрешение на использование идентификатора контактного лица для конкретного зарегистрированного доменного имени. При этом владельцы контактных данных также соглашаются на открытое/защищенное использование своих данных для этой цели. Однако, если у ранее проверенного ЦКЛ нет обязательных/общедоступных элементов данных, отвечающих требованиям данной цели, такое ЦКЛ невозможно назначить для этой цели при регистрации доменного имени.

№ п/п	Принципы раскрытия данных
	в) Тип владельца регистрации г) Идентификатор контактного лица владельца регистрации (дополнительно определен в разделе V) д) Адрес электронной почты владельца регистрации е) Идентификатор контактного лица по техническим вопросам ж) Идентификатор контактного лица по административным вопросам з) Идентификатор контактного лица по правовым вопросам и) Идентификатор контактного лица по вопросам злоупотреблений к) Идентификатор контактного лица поставщика услуг конфиденциальности/ регистрации через доверенных лиц (является обязательным только в том случае, если тип владельца регистрации = поставщик услуг сохранения конфиденциальности/ регистрации через доверенных лиц) л) Идентификатор контактного лица по коммерческим вопросам (является обязательным только в том случае, если тип владельца регистрации = юридическое лицо)
39.	Для достижения равновесия между простотой и доступностью, если владелец регистрации не указывает обязательное ЦКЛ, владельца регистрации необходимо проинформировать о том, что для данного ЦКЛ будет использоваться личный идентификатор контактного лица владельца регистрации, и элементы данных о владельце регистрации будут опубликованы как данные контактного лица по техническим вопросам, контактного лица по административным вопросам, контактного лица по правовым вопросам и контактного лица по вопросам злоупотреблений. Владелец регистрации может избежать раскрытия этих сведений, указав одного или нескольких сторонних ЦКЛ или обратившись к аккредитованному поставщику услуг сохранения конфиденциальности/ регистрации через доверенных лиц (в этом случае необходимые адреса будут предоставлены поставщиком услуг).
40.	Что касается элементов данных, характерных для конкретного ДВУ, реестр ДВУ должен сформировать и опубликовать политику раскрытия данных (соответствующую этим главным принципам) и нести ответственность за определение разрешенных целей использования любых специфичных для ДВУ защищенных элементов данных.

Итоговая классификация элементов данных

На основе этих принципов в приведенной ниже таблице содержится подробная итоговая классификация каждого рекомендованного ЭРГ элемента данных СКР, с использованием следующих условных обозначений:

- Является ли элемент данных обязательным (M) или необязательным (O) для сбора. Это означает:

  [1] Для данных, полученных от владельцев регистраций,
  «обязательный» (M) означает, что данные обязательно должны запрашиваться регистраторами/проверяющими и предоставляться владельцами регистраций, в то время как «необязательный» (O) означает, что данные обязательно должны запрашиваться регистратором/проверяющим, но владелец регистрации может предоставить или не предоставить их по своему усмотрению, в зависимости от обстоятельств.

  [2] Для данных, полученных от владельцев целевых контактных данных,
  «обязательный» (M) означает, что данные обязательно должны запрашиваться регистраторами/проверяющими и предоставляться владельцами контактных данных, в то время как «необязательный» (O) означает, что данные обязательно должны запрашиваться регистратором/проверяющим, но владелец контактных данных может предоставить или не предоставить их по своему усмотрению, в зависимости от обстоятельств, и

  «рекомендованный» (R) означает, что данные обязательно должны запрашиваться регистратором/проверяющим, но владелец контактных данных может предоставить или не предоставить их по своему усмотрению, в зависимости от обстоятельств, что отражает рекомендации по «наилучшей» и «хорошей» практике[12]

---

[12] В основе рекомендованных наилучших практических методов опубликования различных элементов данных ЦКЛ лежит практический опыт членов ЭРГ. Обязательные элементы представляют собой минимальные технические требования, позволяющие достичь указанных целей. Однако на практике, если для конкретной цели существует способ установления связи (например, веб-форма для сообщений о проблемах, дополнительный адрес электронной почты для связи с техническим персоналом), то такой альтернативный способ используется очень широко и часто является предпочтительным для решения проблем. Этот способ меняется в зависимости от ЦКЛ — например, почтовый адрес более целесообразен для контактного лица по правовым или коммерческим вопросам, и как правило бесполезен для быстрого устранения злоупотреблений или для связи с контактными лицами по техническим вопросам. Таким образом, ЭРГ дала конкретные рекомендации по элементам данных для каждого типа ЦКЛ.

[3] Для данных, предоставленных в СКР реестрами и регистраторами, «обязательный» (M) означает, что данные обязательно должны быть предоставлены реестром/регистратором, в то время как «необязательный» (O) означает, что данные могут быть предоставлены или не предоставлены, в зависимости от обстоятельств.

- Является ли каждый элемент общедоступным (P) [доступным любому лицу, прошедшему или не прошедшему процедуру аутентификации] или защищенным (G) [доступным только авторизованным пользователям и только для разрешенных целей], и могут ли владельцы регистраций изменить этот заданный по умолчанию параметр раскрытия данных (Y/N). Это означает:

  [4] Для данных, полученных от владельцев регистраций,
  P / N — все полученные данные должны быть общедоступными и не могут быть скрыты,
  P / Y — все полученные данные по умолчанию общедоступны, но могут быть скрыты владельцем регистрации,
  G / Y — все полученные данные по умолчанию защищены, но владелец регистрации может сделать их общедоступными на основе осознанного согласия.

  [5] Для данных, предоставленных в СКР реестрами и регистраторами,
  P / N — все предоставленные данные должны быть общедоступными и не могут быть скрыты, в то время как
  G / N — означало бы, что все предоставленные данные должны быть защищены; к этой категории не относятся никакие данные.

  [6] Для данных, полученных от владельцев целевых контактных данных,
  P / N — все полученные данные должны быть общедоступными и не могут быть скрыты,
  P / Y— все полученные данные по умолчанию общедоступны, но могут быть скрыты владельцем контактных данных

Следует обратить внимание, что доступность защищенных элементов данных конкретному пользователю зависит от разрешенных целей. Когда владелец регистрации принимает решение сделать по умолчанию защищенные элементы общедоступными, они становятся доступными всем. Когда владелец регистрации принимает решение сделать по умолчанию общедоступные элементы защищенными, доступ к ним будет ограничен разрешенными целями.

ДАННЫЕ, ПРЕДОСТАВЛЕННЫЕ РЕЕСТРОМ/ РЕГИСТРАТОРОМ	Сбор M или O	Раскрытие По умолчанию P или G	Раскрытие Можно ли изменить?	Примечание см. [3] «Определение сбора» и [5] «Определение раскрытия»
Состояние регистрации	**M**	**P**	**N**	
Делегирование DNSSEC	**O**	**P**	**N**	
Состояние на стороне клиента (регистратор)	**M**	**P**	**N**	Содержит все значения, применимые к доменному имени на уровне регистратора: DeleteProhibited (удаление запрещено), RenewProhibited (обновление запрещено), TransferProhibited (передача запрещена)
Состояние на стороне сервера (реестр)	**M**	**P**	**N**	Отсутствует в CAP, аналогично указанному выше, но на уровне реестра
Регистратор	**M**	**P**	**N**	
Реселлер	**O**	**P**	**N**	
Юрисдикция регистратора	**M**	**P**	**N**	Отсутствует в CAP
Юрисдикция реестра	**M**	**P**	**N**	Отсутствует в CAP
Язык соглашения о регистрации	**M**	**P**	**N**	Отсутствует в CAP
Дата создания	**M**	**P**	**N**	
Дата первоначальной регистрации	**O**	**P**	**N**	Отсутствует в CAP
Дата истечения срока действия регистрации	**M**	**P**	**N**	
Дата обновления	**M**	**P**	**N**	
URL-адрес регистратора	**M**	**P**	**N**	
Идентификатор IANA регистратора	**M**	**P**	**N**	
Адрес электронной почты контактного лица регистратора по вопросам злоупотреблений	**M**	**P**	**N**	
Номер телефона контактного лица регистратора по вопросам злоупотреблений	**M**	**P**	**N**	
URL-адрес сайта Internic для отправки жалоб	**M**	**P**	**N**	

ДАННЫЕ О ВЛАДЕЛЬЦЕ РЕГИСТРАЦИИ полученные от владельца регистрации	Сбор M или O	Раскрытие По умолчанию P или G	Раскрытие Можно ли изменить?	Примечание см. [1] «Определение сбора» и [4] «Определение раскрытия»
Доменное имя	**M**	**P**	**N**	
Серверы DNS	**M**	**P**	**N**	
Имя владельца регистрации	**M**	**G**	**Y**	
Тип владельца регистрации	**M**	**P**	**N**	
Идентификатор контактного лица владельца регистрации	**M**	**P**	**N**	Заменяет идентификатор владельца регистрации в реестре, выданный проверяющим в СКР
Статус подтверждения контактного лица владельца регистрации	**M**	**P**	**N**	Новый, указанный проверяющим
Метка времени последнего подтверждения контактного лица владельца регистрации	**M**	**P**	**N**	Новый, указанный проверяющим
Организация владельца регистрации	**O**	**P**	**Y**	Данные регистрируются, когда тип владельца регистрации = юридическое лицо или поставщик услуг сохранения конфиденциальности
Идентификатор компании, являющейся владельцем регистрации (например, фирменное название, номер D-U-Нет-S)	**O**	**P**	**Y**	Идентификаторы реального мира, выданные компаниям такими источниками, как Dunn and Bradstreet Сбор осуществляется, когда Тип владельца регистрации = Юридическое лицо Отсутствует в CAP
Уличный адрес владельца регистрации	**M**	**G**	**Y**	
Город владельца регистрации	**M**	**G**	**Y**	
Регион/штат владельца регистрации	**O**	**G**	**Y**	В соответствии с CAP 2013, сбор всех элементов «Штат/Регион» осуществляется, когда это применимо

Почтовый индекс владельца регистрации	**O**	**G**	**Y**	В соответствии с CAP 2013, сбор всех элементов «Почтовый индекс» осуществляется, когда это применимо
Страна владельца регистрации	**M**	**G**	**Y**	
Телефонный номер владельца регистрации + добавочный номер	**M**	**G**	**Y**	Сбор добавочных номеров осуществляется в случае необходимости
Альтернативный телефонный номер владельца регистрации + добавочный номер	**O**	**G**	**Y**	Новый пункт, отсутствует в CAP
Адрес электронной почты владельца регистрации	**M**	**P**	**N**	
Альтернативный адрес электронной почты владельца регистрации	**O**	**P**	**Y**	Новый пункт, отсутствует в CAP
Номер факса владельца регистрации + добавочный номер	**O**	**G**	**Y**	В соответствии с CAP 2013, сбор всех элементов «Факс» и «Доб. факс» осуществляется, когда это применимо
Данные для отправки владельцу регистрации SMS	**O**	**G**	**Y**	Новый пункт, отсутствует в CAP
Данные для отправки владельцу регистрации мгновенных сообщений	**O**	**G**	**Y**	Новый пункт, отсутствует в CAP
Идентификатор владельца регистрации в социальной сети	**O**	**G**	**Y**	Новый пункт, отсутствует в CAP
Альтернативный идентификатор владельца регистрации в социальной сети	**O**	**G**	**Y**	Новый пункт, отсутствует в CAP
URL-адрес контактного лица владельца регистрации	**O**	**G**	**Y**	Новый пункт, отсутствует в CAP
URL-адрес контактного лица владельца регистрации по вопросам злоупотреблений	**O**	**G**	**Y**	Новый пункт, отсутствует в CAP

ЦЕЛЕВЫЕ КОНТАКТНЫЕ ЛИЦА Представитель администратора	Сбор M/R/O	Раскрытие По умолчанию P или G	Раскрытие Можно ли изменить?	Примечание см. [2] «Определение сбора» и [6] «Определение раскрытия»
Цели: Покупка и продажа ДИ, управление доменным именем, исследование DNS				
Идентификатор контактного лица по административным вопросам	**M**	**P**	**N**	
Идентификатор ЦКЛ	**M**	**P**	**N**	Отсутствует в CAP
Статус подтверждения ЦКЛ	**M**	**P**	**N**	Новый, указанный проверяющим
Метка времени последнего подтверждения ЦКЛ	**M**	**P**	**N**	Новый, указанный проверяющим
Имя ЦКЛ	**M**	**P**	**N**	
Организация ЦКЛ	**M**	**P**	**N**	
Уличный адрес ЦКЛ	**R**	**P**	**Y**	
Город ЦКЛ	**R**	**P**	**Y**	
Регион/штат ЦКЛ	**O**	**P**	**Y**	
Почтовый индекс ЦКЛ	**O**	**P**	**Y**	
Страна ЦКЛ	**M**	**P**	**N**	
Телефонный номер ЦКЛ + добавочный номер	**O**	**P**	**Y**	
Альтернативный телефонный номер ЦКЛ + добавочный номер	**O**	**P**	**Y**	Отсутствует в CAP
Адрес электронной почты ЦКЛ	**M**	**P**	**N**	
Альтернативный адрес электронной почты ЦКЛ	**O**	**P**	**Y**	Отсутствует в CAP
Номер факса ЦКЛ + добавочный номер	**O**	**P**	**Y**	
Данные для отправки ЦКЛ SMS	**O**	**P**	**Y**	Отсутствует в CAP
Данные для отправки ЦКЛ мгновенных сообщений	**O**	**P**	**Y**	Отсутствует в CAP
Идентификатор ЦКЛ в социальной сети	**O**	**P**	**Y**	Отсутствует в CAP
Альтернативный идентификатор ЦКЛ в социальной сети	**O**	**P**	**Y**	Отсутствует в CAP
URL-адрес ЦКЛ	**O**	**P**	**Y**	Отсутствует в CAP
URL-адрес ЦКЛ по вопросам злоупотреблений	**O**	**P**	**Y**	Отсутствует в CAP

ЦЕЛЕВЫЕ КОНТАКТНЫЕ ЛИЦА Контактное лицо по правовым вопросам	**Сбор M/R/O**	**Раскрытие По умолчанию P или G**	**Раскрытие Можно ли изменить?**	**Примечание** см. [2] «Определение сбора» и [6] «Определение раскрытия»
Цели: юридические действия, соблюдение нормативных и договорных обязательств Исследование DNS в научных или общественных интересах				
Идентификатор контактного лица по правовым вопросам	**M**	**P**	**N**	Отсутствует в CAP
Идентификатор ЦКЛ	**M**	**P**	**N**	Отсутствует в CAP
Статус подтверждения ЦКЛ	**M**	**P**	**N**	Новый, указанный проверяющим
Метка времени последнего подтверждения ЦКЛ	**M**	**P**	**N**	Новый, указанный проверяющим
Имя ЦКЛ	**M**	**P**	**N**	
Организация ЦКЛ	**M**	**P**	**N**	
Уличный адрес ЦКЛ	**M**	**P**	**N**	
Город ЦКЛ	**M**	**P**	**N**	
Регион/штат ЦКЛ	**O**	**P**	**Y**	
Почтовый индекс ЦКЛ	**O**	**P**	**Y**	
Страна ЦКЛ	**M**	**P**	**N**	
Телефонный номер ЦКЛ + добавочный номер	**M**	**P**	**N**	
Альтернативный телефонный номер ЦКЛ + добавочный номер	**O**	**P**	**Y**	Отсутствует в CAP
Адрес электронной почты ЦКЛ	**M**	**P**	**N**	
Альтернативный адрес электронной почты ЦКЛ	**O**	**P**	**Y**	Отсутствует в CAP
Номер факса ЦКЛ + добавочный номер	**R**	**P**	**Y**	
Данные для отправки ЦКЛ SMS	**O**	**P**	**Y**	Отсутствует в CAP
Данные для отправки ЦКЛ мгновенных сообщений	**O**	**P**	**Y**	Отсутствует в CAP
Идентификатор ЦКЛ в социальной сети	**O**	**P**	**Y**	Отсутствует в CAP
Альтернативный идентификатор ЦКЛ в социальной сети	**O**	**P**	**Y**	Отсутствует в CAP
URL-адрес ЦКЛ	**O**	**P**	**Y**	Отсутствует в CAP
URL-адрес ЦКЛ по вопросам злоупотреблений	**O**	**P**	**Y**	Отсутствует в CAP

ЦЕЛЕВЫЕ КОНТАКТНЫЕ ЛИЦА Контактное лицо по техническим вопросам	Сбор M/R/O	Раскрытие По умолчанию P или G	Раскрытие Можно ли изменить?	Примечание см. [2] «Определение сбора» и [6] «Определение раскрытия»
Цели: решение технических проблем, управление доменным именем, исследование DNS				
Идентификатор контактного лица по техническим вопросам	**M**	**P**	**N**	
Идентификатор ЦКЛ	**M**	**P**	**N**	Отсутствует в CAP
Статус подтверждения ЦКЛ	**M**	**P**	**N**	Новый, указанный проверяющим
Метка времени последнего подтверждения ЦКЛ	**M**	**P**	**N**	Новый, указанный проверяющим
Имя ЦКЛ	**R**	**P**	**Y**	
Организация ЦКЛ	**R**	**P**	**Y**	
Уличный адрес ЦКЛ	**R**	**P**	**Y**	
Город ЦКЛ	**R**	**P**	**Y**	
Регион/штат ЦКЛ	**O**	**P**	**Y**	
Почтовый индекс ЦКЛ	**O**	**P**	**Y**	
Страна ЦКЛ	**M**	**P**	**N**	
Телефонный номер ЦКЛ + добавочный номер	**R**	**P**	**Y**	
Альтернативный телефонный номер ЦКЛ + добавочный номер	**R**	**P**	**Y**	Отсутствует в CAP
Адрес электронной почты ЦКЛ	**M**	**P**	**N**	
Альтернативный адрес электронной почты ЦКЛ	**R**	**P**	**Y**	Отсутствует в CAP
Номер факса ЦКЛ + добавочный номер	**O**	**P**	**Y**	
Данные для отправки ЦКЛ SMS	**R**	**P**	**Y**	Отсутствует в CAP
Данные для отправки ЦКЛ мгновенных сообщений	**R**	**P**	**Y**	Отсутствует в CAP
Идентификатор ЦКЛ в социальной сети	**O**	**P**	**Y**	Отсутствует в CAP
Альтернативный идентификатор ЦКЛ в социальной сети	**O**	**P**	**Y**	Отсутствует в CAP
URL-адрес ЦКЛ	**R**	**P**	**Y**	Отсутствует в CAP
URL-адрес ЦКЛ по вопросам злоупотреблений	**O**	**P**	**Y**	Отсутствует в CAP

ЦЕЛЕВЫЕ КОНТАКТНЫЕ ЛИЦА Контактное лицо по вопросам злоупотреблений	Сбор M/R/O	Раскрытие По умолчанию P или G	Раскрытие Можно ли изменить?	Примечание см. [2] «Определение сбора» и [6] «Определение раскрытия»
Цель: предотвращение злоупотреблений, управление доменным именем, исследование DNS				
Идентификатор контактного лица по вопросам злоупотреблений	**M**	**P**	**N**	Отсутствует в CAP
Идентификатор ЦКЛ	**M**	**P**	**N**	Отсутствует в CAP
Статус подтверждения ЦКЛ	**M**	**P**	**N**	Новый, указанный проверяющим
Метка времени последнего подтверждения ЦКЛ	**M**	**P**	**N**	Новый, указанный проверяющим
Имя ЦКЛ	**R**	**P**	**Y**	
Организация ЦКЛ	**R**	**P**	**Y**	
Уличный адрес ЦКЛ	**R**	**P**	**Y**	
Город ЦКЛ	**R**	**P**	**Y**	
Регион/штат ЦКЛ	**O**	**P**	**Y**	
Почтовый индекс ЦКЛ	**O**	**P**	**Y**	
Страна ЦКЛ	**M**	**P**	**N**	
Телефонный номер ЦКЛ + добавочный номер	**M**	**P**	**N**	
Альтернативный телефонный номер ЦКЛ + добавочный номер	**O**	**P**	**Y**	Отсутствует в CAP
Адрес электронной почты ЦКЛ	**M**	**P**	**N**	
Альтернативный адрес электронной почты ЦКЛ	**O**	**P**	**Y**	Отсутствует в CAP
Номер факса ЦКЛ + добавочный номер	**O**	**P**	**Y**	
Данные для отправки ЦКЛ SMS	**O**	**P**	**Y**	Отсутствует в CAP
Данные для отправки ЦКЛ мгновенных сообщений	**R**	**P**	**Y**	Отсутствует в CAP
Идентификатор ЦКЛ в социальной сети	**R**	**P**	**Y**	Отсутствует в CAP
Альтернативный идентификатор ЦКЛ в социальной сети	**O**	**P**	**Y**	Отсутствует в CAP
URL-адрес ЦКЛ	**R**	**P**	**Y**	Отсутствует в CAP
URL-адрес ЦКЛ по вопросам злоупотреблений	**R**	**P**	**Y**	Отсутствует в CAP

ЦЕЛЕВЫЕ КОНТАКТНЫЕ ЛИЦА Контактное лицо поставщика услуг сохранения конфиденциальности/ регистрации через доверенных лиц (КД)	**Сбор M/R/O**	**Раскрытие По умолчанию P или G**	**Раскрытие Можно ли изменить?**	**Примечание** см. [2] «Определение сбора» и [6] «Определение раскрытия»
Цели: защита персональных данных, управление доменным именем, исследование DNS				
Идентификатор контактного лица КД	**M**	**P**	**N**	Отсутствует в CAP
Идентификатор ЦКЛ	**M**	**P**	**N**	Отсутствует в CAP
Статус подтверждения ЦКЛ	**M**	**P**	**N**	Новый, указанный проверяющим
Метка времени последнего подтверждения ЦКЛ	**M**	**P**	**N**	Новый, указанный проверяющим
Имя ЦКЛ	**M**	**P**	**N**	
Организация ЦКЛ	**M**	**P**	**N**	
Уличный адрес ЦКЛ	**M**	**P**	**N**	
Город ЦКЛ	**M**	**P**	**N**	
Регион/штат ЦКЛ	**O**	**P**	**Y**	
Почтовый индекс ЦКЛ	**O**	**P**	**Y**	
Страна ЦКЛ	**M**	**P**	**N**	
Телефонный номер ЦКЛ + добавочный номер	**M**	**P**	**N**	
Альтернативный телефонный номер ЦКЛ + добавочный номер	**O**	**P**	**Y**	Отсутствует в CAP
Адрес электронной почты ЦКЛ	**M**	**P**	**N**	
Альтернативный адрес электронной почты ЦКЛ	**O**	**P**	**Y**	Отсутствует в CAP
Номер факса ЦКЛ + добавочный номер	**O**	**P**	**Y**	
Данные для отправки ЦКЛ SMS	**O**	**P**	**Y**	Отсутствует в CAP
Данные для отправки ЦКЛ мгновенных сообщений	**O**	**P**	**Y**	Отсутствует в CAP
Идентификатор ЦКЛ в социальной сети	**O**	**P**	**Y**	Отсутствует в CAP
Альтернативный идентификатор ЦКЛ в социальной сети	**O**	**P**	**Y**	Отсутствует в CAP
URL-адрес ЦКЛ	**M**	**P**	**N**	Отсутствует в CAP
URL-адрес ЦКЛ по вопросам злоупотреблений	**M**	**P**	**N**	Отсутствует в CAP

ЦЕЛЕВЫЕ КОНТАКТНЫЕ ЛИЦА Контактное лицо по коммерческим вопросам	Сбор M/R/O	Раскрытие По умолчанию P или G	Раскрытие Можно ли изменить?	Примечание см. [2] «Определение сбора» и [6] «Определение раскрытия»
Цели: индивидуальное использование Интернета, управление доменным именем, исследование DNS				
Идентификатор контактного лица по коммерческим вопросам	**M**	**P**	**N**	Отсутствует в CAP
Идентификатор ЦКЛ	**M**	**P**	**N**	Отсутствует в CAP
Статус подтверждения ЦКЛ	**M**	**P**	**N**	Новый, указанный проверяющим
Метка времени последнего подтверждения ЦКЛ	**M**	**P**	**N**	Новый, указанный проверяющим
Имя ЦКЛ	**M**	**P**	**N**	
Организация ЦКЛ	**M**	**P**	**N**	
Уличный адрес ЦКЛ	**M**	**P**	**N**	
Город ЦКЛ	**M**	**P**	**N**	
Регион/штат ЦКЛ	**O**	**P**	**Y**	
Почтовый индекс ЦКЛ	**O**	**P**	**Y**	
Страна ЦКЛ	**M**	**P**	**N**	
Телефонный номер ЦКЛ + добавочный номер	**R**	**P**	**Y**	
Альтернативный телефонный номер ЦКЛ + добавочный номер	**O**	**P**	**Y**	Отсутствует в CAP
Адрес электронной почты ЦКЛ	**R**	**P**	**Y**	
Альтернативный адрес электронной почты ЦКЛ	**O**	**P**	**Y**	Отсутствует в CAP
Номер факса ЦКЛ + добавочный номер	**O**	**P**	**Y**	
Данные для отправки ЦКЛ SMS	**O**	**P**	**Y**	Отсутствует в CAP
Данные для отправки ЦКЛ мгновенных сообщений	**O**	**P**	**Y**	Отсутствует в CAP
Идентификатор ЦКЛ в социальной сети	**O**	**P**	**Y**	Отсутствует в CAP
Альтернативный идентификатор ЦКЛ в социальной сети	**O**	**P**	**Y**	Отсутствует в CAP
URL-адрес ЦКЛ	**R**	**P**	**Y**	Отсутствует в CAP
URL-адрес ЦКЛ по вопросам злоупотреблений	**O**	**P**	**Y**	Отсутствует в CAP

ЭРГ также повторяет свою рекомендацию о выполнении широкого анализа рисков/последствий с целью подтверждения того, что эта классификация на основе принципов действительно приведет к надлежащему сбору и раскрытию данных для определенных целей.

Приведение в соответствие с CAP 2013 и новыми элементами данных

Чтобы способствовать переходу и пониманию, рекомендованные ЭРГ названия элементов данных по-возможности были приведены в соответствие с указанными в CAP 2013 (например, Делегирование DNSSEC, Дата истечения срока действия СКР). Однако названий элементов данных, которые используются в CAP 2013 для элементов контактных данных, не хватает для отражения предложения ЭРГ по целевым контактным лицам (см. раздел III). Для устранения этого ЭРГ применила следующие сопоставления:

> Когда идентификатор контактного лица по административным вопросам в СКР относится к ЦКЛ,
> Имя ЦКЛ в СКР = Имя контактного лица по административным вопросам в CAP
> Организация ЦКЛ в СКР = Организация контактного лица по административным вопросам в CAP
> и так далее для остальных элементов данных контактного лица по административным вопросам в CAP
>
> Когда идентификатор контактного лица по техническим вопросам в СКР относится к ЦКЛ,
> Имя ЦКЛ в СКР = Имя контактного лица по техническим вопросам в CAP
> Организация ЦКЛ в СКР = Организация контактного лица по техническим вопросам в CAP
> и так далее для остальных элементов данных контактного лица по техническим вопросам в CAP

Примечание: ЭРГ рекомендует на портале СКР предусмотреть легкодоступные для пользователей СКР определения каждого типа ЦКЛ (например, использовать всплывающие при наведении курсора подсказки), чтобы четко указать, что данные ЦКЛ публикуются для использования в разрешенных целях, и данную точку контакта необходимо назначить для охвата указанных целей. Владельцы регистраций имеют право принять решение о получении запросов лично (указать в качестве ЦКЛ идентификатор владельца регистрации), задействовать для получения этих запросов поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц (воспользоваться для этих элементов данных сведениями, которые предоставит

поставщик КД — как правило, адресами для пересылки или адресами поставщика) или указать конкретную организацию, которая будет получать эти запросы (например, поставщика услуг, поставщика хостинга, законного представителя, службу поддержки клиентов).

Все элементы данных соответствуют тем, которые определены в CAP 2013, со следующими добавлениями:

Юрисдикция регистраторов и реестров: правовая юрисдикция, в которой работает регистратор или реестр, которая указана в подписанном ими соглашении с ICANN.

Язык соглашения о регистрации: язык на котором оформлен договор регистратора с владельцем регистрации.

Дата первоначальной регистрации: дата первой регистрации доменного имени.[13]

Состояние на стороне клиента, состояние на стороне сервера: расширяя значения состояния на стороне клиента CAP 2013, эти элементы данных содержат значения состояния на стороне регистратора (клиента) и реестра (сервера), которые в настоящее время применимы к этому доменному имени: DeleteProhibited (удаление запрещено), RenewProhibited (обновление запрещено), TransferProhibited (передача запрещена).

Идентификатор компании, являющейся владельцем регистрации: Торговый номер Великобритании, номер D-U-N-S или другой уникальный идентификатор компании в реальном мире, присвоенный владельцу регистрации в открытом реестре коммерческих лиц. Этот элемент данных позволяет осуществлять поиск компании за рамками СКР.

Идентификатор контактного лица владельца регистрации: уникальный маркер, присвоенный предварительно проверенному блоку контактных данных, которые идентифицируют владельца регистрации данного доменного имени. Более подробное определение идентификатора контактного лица, а также процесса его создания и использования см. в разделе V. Этот идентификатор позволяет многократно использовать и обслуживать контактные данные в СКР. Следует обратить внимание, что когда Тип владельца регистрации = Поставщик услуг защиты конфиденциальности и регистрации через доверенных лиц,

[13] Эта дата отличается от даты создания, поскольку дата создания фиксирует дату последней регистрации доменного имени; возможно, что данное доменное имя ранее неоднократно регистрировалось и удалялось. Дата первоначальной регистрации обозначает дату первой регистрации этого доменного имени.

идентификатором контактного лица владельца регистрации будет уникальный идентификатор, назначенный этому аккредитованному поставщику.

Статус подтверждения контактных данных владельца регистрации/ЦКЛ, Метка времени последнего подтверждения контактных данных владельца регистрации/ЦКЛ: достигнутый максимальный уровень подтверждения и дата последнего подтверждения, которые дополнительно определены в разделе V.

Адрес владельца регистрации/ЦКЛ для отправки SMS, мгновенных сообщений и в социальной сети: новые способы связи, которые могут дополнительно применяться для установления контакта с владельцем регистрации или ЦКЛ путем отправки SMS, обмена мгновенными сообщениями или с помощью другого альтернативного средства связи через социальную сеть.

Альтернативный адрес электронной почты, альтернативный телефон, альтернативная социальная сеть владельца регистрации/ЦКЛ: новые альтернативные адреса, которые могут дополнительно применяться для установления контакта с владельцем регистрации или ЦКЛ при невозможности связаться по основному адресу. Эти новые элементы данных предназначены для удовлетворения распространенных потребностей, например для решения технических проблем в ситуации, когда доменное имя не функционирует, и для ускорения связи по мобильному телефону или через социальную сеть.

URL-адрес для контактов и URL-адрес для контактов по вопросам злоупотреблений владельца регистрации/ЦКЛ: новые необязательные элементы данных, которые позволяют перейти на веб-страницы, где можно разместить инструкции по отправке сообщений или информации о злоупотреблениях, политики или формы, способствующие более продуктивной связи.

Идентификатор контактного лица ЦКЛ: уникальный маркер, присвоенный предварительно проверенному блоку контактных данных, которые идентифицируют ЦКЛ данного доменного имени, выполняющего функцию, определяемую элементом данных Функция контактного лица. Идентификатор контактного лица владельца регистрации и идентификатор контактного лица ЦКЛ могут указывать на одно и то же лицо или на разных лиц.

Примечание: перед реализацией любой системы СКР необходимо рассмотреть трудности перехода и соблюдения обязательств, связанные с этими новыми элементами.

б. Принципы нерегулируемого и регулируемого доступа к данным

ЭРГ рекомендует внедрить новый подход для доступа к регистрационным данным, полностью отказавшись от анонимного доступа кого-либо к чему-либо в пользу новой парадигмы, в которой открытый доступ к некоторым данным сочетается с регулируемым доступом к остальным данным. Ниже приведены принципы, отражающие эту рекомендацию.

№ п/п	Принципы доступа к данным
41.	Минимальный набор элементов данных, по крайней мере соответствующий наиболее строгому режиму конфиденциальности, должен быть доступен для пользователей СКР без необходимости авторизации.
42.	Необходимо обеспечить поддержку нескольких уровней авторизованного доступа к данным, в соответствии со сформулированными разрешенными целями.
43.	Используемые для доступа к СКР учетные данные пользователей необходимо связать с доступной для проверки процедурой аккредитации, как дополнительно определено в разделе IV(c), «Аккредитация пользователей СКР».
44.	Доступ должен предоставляться на недискриминационной основе (т. е. процедура должна создавать равные условия для всех подателей запросов, преследующих одну и ту же цель).
45.	Чтобы препятствовать злоупотреблениям и способствовать подотчетности: • доступ ко всем элементам данных должен предоставляться на основе заявленной цели; • доступ к защищенным элементам данных должен быть ограничен кругом авторизованных инициаторов запросов, которые заявили о своей разрешенной цели; и • инициаторы запросов должны иметь возможность подать заявку и получить учетные данные для их использования при последующем авторизованном доступе к запросам на получение данных.

№ п/п	Принципы доступа к данным
46.	Инициаторы запросов на авторизованный доступ должны проходить некоторую аккредитацию: • При запросе данных аккредитованным лицом, цель подателя запроса должна быть указана при каждом новом запросе. • Для разных целей могут применяться различные условия и положения. • В случае нарушения аккредитованным подателем запросов условий и положений должны применяться штрафные санкции.
47.	Чтобы повысить уровень защиты регистрационных данных рДВУ, для всех запросов и ответов СКР необходимо использовать общедоступные способы шифрования и проверки подлинности сообщений с целью защиты конфиденциальности и целостности передаваемых данных.
48.	Для удовлетворения потребностей авторизованных пользователей СКР с разрешенными целями СКР обязана предоставлять услугу «Обратный запрос», которая обеспечивает поиск открытых и защищенных элементов данных по конкретному значению и возвращает список доменных имен, в которых упоминается это значение.
49.	Для удовлетворения потребностей авторизованных пользователей СКР с разрешенными целями СКР обязана предоставлять услугу «WhoWas», которая возвращает архивные мгновенные снимки открытых и защищенных элементов для конкретных доменных имен, ограничиваясь при этом данными, которые имеются в СКР.
50.	СКР должна поддерживать инновационные услуги, которые позволяют воспользоваться элементами данных СКР следующим образом. • Третьи стороны должны иметь возможность оказания существующих и будущих инновационных услуг, — в том числе обратных запросов и услуг WhoWas, — используя для этого общедоступные элементы данных и соблюдая условия и положения использования данных СКР. • В тех случаях, когда третьи стороны предлагают инновационные услуги с использованием защищенных элементов данных, эти третьи стороны обязаны получить аккредитацию и соблюдать условия и положения использования данных СКР.

№ п/п	Принципы доступа к данным
51.	Раскрытие всех защищенных элементов данных должно осуществляться в рамках установленных способов доступа к СКР (включая описанные выше). Полный набор данных СКР для всех рДВУ (или полный набор данных реестра для отдельного рДВУ) не должен экспортироваться в массовом порядке путем неконтролируемого доступа.
52.	Раскрытие данных может осуществляться путем их интерактивного отображения и других способов доступа к СКР. • Чтобы упростить поиск данных и единообразный доступ к ним, необходимо предложить центральную точку доступа (например, веб-портал). • Безопасный доступ к общедоступным данным должен предоставляться всем инициаторам запросов с использованием отправки незаверенных запросов (как минимум, через защищенный веб-сайт). • Безопасный доступ к закрытым данным должен поддерживаться с использованием безопасных веб-технологий и других методов и форматов доступа (например, XML-ответы RDAP, SMS, электронная почта) на основе авторизации инициатора запроса и с учетом цели запроса. • Инициаторы запросов должны иметь возможность в случае необходимости получить достоверные данные из СКР в режиме реального времени. • СКР должна предусматривать возможность автоматизации широкомасштабных операций поиска для различных сценариев использования и разрешенных целей.
53.	Чтобы стать по-настоящему международной, СКР должна обеспечивать отображение регистрационных данных на нескольких языках, с использованием нескольких систем письменности и алфавитов, включая интернационализированные доменные имена (ИДИ).
54.	Следует предусмотреть в СКР поддержку всех будущих политик транслитерации для рДВУ, сформулированных ОПРИ.
55.	Следует предусмотреть в СКР возможность сбора и отображения элементов регистрационных данных на местных языках.

Пример открытого доступа к данным

Как изображено на следующей иллюстрации, открытые элементы данных могут быть по-прежнему запрошены из СКР любым лицом, прошедшим или не прошедшим процедуру аутентификации. Более подробный пример элементов данных, отправленных в ответ на незаверенный запрос открытых данных, см. в Приложении E ANNEX A: .

Рис. 6. Нерегулируемый доступ к открытым регистрационным данным через СКР

Приложение I ANNEX A: также содержит блок-схемы и пример использования для демонстрации этапов доступа к соответствующим элементам данных.

Пример регулируемого доступа к данным

Как показано на следующей иллюстрации, защищенные элементы данных тоже можно запрашивать через СКР. Для этого инициатор запроса сначала должен быть аккредитован. После этого инициаторы запросов могут отправлять заверенные запросы на получение элементов данных для заявленной цели. Более подробный пример элементов данных, отправленных в ответ на заверенный запрос защищенных данных, см. в Приложении E ANNEX A: .

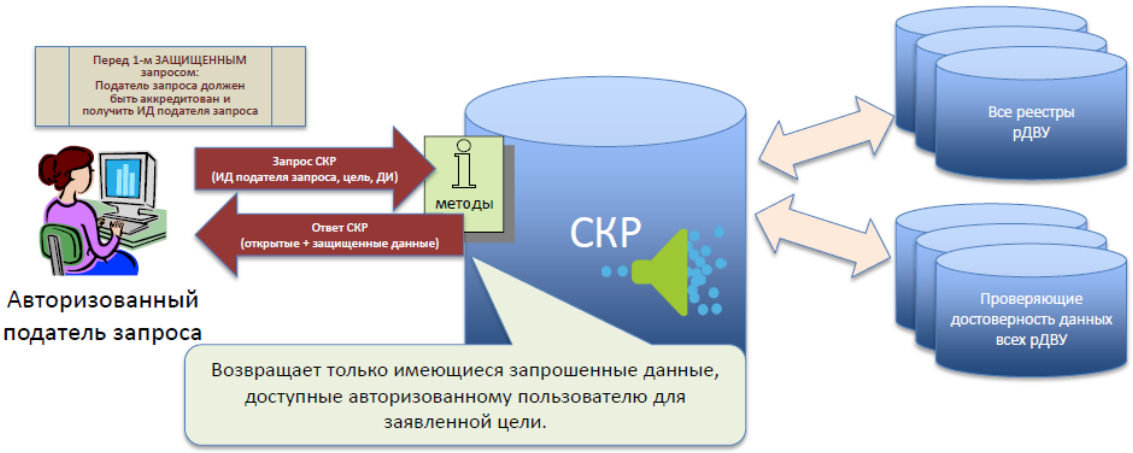


Рис. 7. Регулируемый доступ к регистрационным данным через СКР

Технические протоколы и методы доступа

ЭРГ изучила возможность поддержки рекомендованных группой характеристик проекта техническими протоколами, внедренными в сегодняшней системе регистрации доменных имен (например, EPP[14]) и находящимися на стадии разработки в IETF (например, рассматриваемыми рабочей группой WEIRDs). Группа WEIRDs скоро завершит разработку нового стандарта, который называется «Протокол доступа к регистрационным данным» (Registration Data Access Protocol — RDAP). Внедрение этих протоколов для рекомендованной ЭРГ модели может привести к снижению расходов на переход для всех затрагиваемых сторон.

ЭРГ проанализировала возможность поддержки протоколом EPP каждого элемента данных, включенного в рекомендованную группой СКР, и возможность поддержки протоколом RDAP рекомендованных ЭРГ принципов использования учетных данных для доступа. Выполненный ЭРГ анализ позволяет предположить, что как EPP, так и RDAP могут использоваться СКР, независимо от того, какая из альтернативных моделей будет выбрана. Однако для этого могут потребоваться несколько расширений, дополнений или применение «примечаний» RDAP. Подробная оценка каждого из этих протоколов включена в Приложение G.

в. Принципы аккредитации пользователей СКР

Как отмечалось в разделе III «Цели», для некоторых целей необходим доступ ко всем защищенным элементам или к разрешенному для использования подмножеству защищенных элементов данных. Как отмечалось в разделе IV(b)

[14] См. EPP: стандарт 69, документы RFC 5730–5734

«Принцип № 46», любая цель, для которой необходим доступ к защищенным данным, требует аккредитации пользователя. Однако аккредитация пользователя не подразумевает неограниченного доступа ко всем защищенным данным. Доступ должен быть основан на целях, возвращая в ответ на запросы только те элементы данных, которые разрешены для заявленной цели.

ЭРГ рекомендует для каждого указанного в разделе III сообщества пользователей СКР, желающего получить доступ к защищенным данным для разрешенных целей, проконсультироваться с экспертами сообщества для подтверждения того, что группа ЭРГ правильно определила цели использования регистрационных данных, элементы данных, которые должны быть доступными для этих целей, и возможные органы аккредитации пользователей СКР.

Вероятно, многие организации заключат с ICANN договора на выполнение функций органов аккредитации пользователей СКР. Хотя все органы аккредитации пользователей СКР должны соблюдать общий набор принципов, для каждого сообщества пользователей СКР возможны свои решения по реализации. Например:

Сценарий № 1. Орган аккредитации, независимый от оператора аккредитации, когда орган утверждает пользователей, а сторонний оператор управляет доступом аккредитованных пользователей к СКР

В таком сообществе пользователей СКР, как владельцы товарных знаков, отраслевая организация может взять на себя ответственность за аккредитацию своих собственных членов, желающих получить доступ к защищенным данным для разрешенных целей. Этот орган аккредитации может не играть никакой роли в управлении учетными записями пользователей или в авторизации запросов на получение доступа, отправляемых СКР. Вместо этого, орган аккредитации устанавливает правила членства и условия предоставления услуг, осуществляет процедуры рассмотрения заявок и обеспечения соблюдения требований и т. п. для данного сообщества пользователей СКР. Орган аккредитации может заключить договор со сторонним оператором аккредитации, который будет создавать учетные записи пользователей СКР и управлять ими, выдавать учетные данные для доступа к СКР, осуществлять авторизацию запросов на доступ к СКР и обработку сообщений о злоупотреблениях первого уровня, включая временную приостановку действия учетной записи. Оператор аккредитации просто обеспечивает реализацию и соблюдение правил доступа к СКР, установленных органом аккредитации для данного сообщества; любые претензии в связи с приостановкой действия учетной записи или другие споры будут передаваться для разрешения органу аккредитации.

Сценарий № 2. Орган аккредитации, объединенный с оператором аккредитации, передающий запросы на авторизацию доступа в СКР.

В таком сообществе пользователей СКР, как службы безопасности, отраслевая организация может взять на себя ответственность за аккредитацию своих собственных членов в соответствии с (утвержденной) процедурой, которую она уже использует для предоставления пользователям доступа к другим системам. В этом примере организация выступает и в качестве органа аккредитации, и в качестве оператора аккредитации, с максимальным привлечением существующей системы, которая уже используется членами этого сообщества для авторизации доступа, и передачей в СКР запросов на получение доступа к защищенным данным для разрешенных целей. В данном случае пользователь СКР несет ответственность за соблюдение условий и положений, а отраслевая организация обязана ввести процедуру для случаев злоупотребления доступом, приостановки доступа и т. п., применяемую для операций доступа к СКР конкретного пользователя.

Сценарий № 3. Орган аккредитации, объединенный с оператором аккредитации, передающий запросы своих членов в СКР от своего имени (то есть модель Интерпола).

В таком сообществе пользователей СКР, как правоохранительные органы, заслуживающая доверия организация может взять на себя ответственность за аккредитацию своих собственных членов в соответствии с (утвержденной) процедурой, которую она уже использует для предоставления пользователям доступа к другим системам. В этом примере организация выступает и в качестве органа аккредитации, и в качестве оператора аккредитации, с максимальным привлечением существующей системы, которая уже используется членами этого сообщества для авторизации доступа, и передачей в СКР запросов на получение доступа к защищенным данным для разрешенных целей от своего имени. В данном случае пользователем СКР является организация, которая берет на себя ответственность за действия своих членов, направляя их запросы от своего имени, и за соблюдение условий и положений. Хотя СКР может не располагать сведениями о действиях конкретного пользователя, указанная организация обязана ввести такую процедуру для случаев злоупотребления доступом, приостановки доступа и т. п., которая позволит организации проверять операции доступа конкретных пользователей и выявлять злоупотребления.

Чтобы обеспечить возможность доступа аккредитованных пользователей СКР к защищенным элементам данных для разрешенных целей, ЭРГ рекомендует применять следующие принципы аккредитации пользователей СКР.

№ п/п	Принципы аккредитации пользователей СКР
56.	Доступ не аккредитованных пользователей без проверки подлинности к незащищенным (то есть общедоступным) данным должен быть возможен в режиме реального времени.
57.	Аккредитация пользователей СКР для доступа к данным СКР не должна происходить в режиме реального времени для всех сценариев применения и/или инициаторов запросов.
58.	СКР обязана применять только минимальную «схему аккредитации», необходимую для предоставления пользователю СКР доступа к защищенным элементам данных для заявленной цели.[15]
59.	Требование «заранее получить разрешение» или ввести учетные данные не должно предъявляться каждому потенциальному пользователю СКР. Можно создать процедуру отправки и выполнения запросов для каждого «типа» аккредитованных пользователей СКР (то есть для сообщества пользователей СКР).
60.	Аккредитацию пользователей СКР, стремящихся получить доступ к данным для разрешенных целей, можно осуществлять тремя способами. • Без аккредитации (то есть предоставлять доступ только к общедоступным данным без проверки подлинности, как описано выше). • Самоаккредитация физического или юридического лица, запрашивающего данные, например система, в которой пользователи просто вводят сведения о себе, о том, какие данные они запрашивают, и затем им предоставляется доступ к этому уровню данных. Например, это может применяться к владельцам регистрации, которым необходим доступ к данным о собственном доменном имени для целей управления доменным именем, когда их самоаттестация привязана к реальной регистрации доменного имени, которая дает право на получение учетных данных для доступа к этой информации в СКР. • Аккредитация, которой занимается заслуживающая доверия третья сторона (то есть орган аккредитации пользователей СКР, см. принцип № 64 ниже).

[15] Например, эта аккредитация не должна требовать многофакторных, юридически заверенных заявлений или служить системой чрезвычайной важности для получения большинства типов данных.

№ п/п	Принципы аккредитации пользователей СКР
61.	Во всех возможных случаях, для любой процедуры аккредитации в СКР, используемой третьей стороной, в ситуации, требующей получения учетных данных, следует максимально эффективно пользоваться процедурами аккредитации, которые уже есть в каждом сообществе пользователей СКР, указанном в разделе III.
62.	Эти сторонние процедуры аккредитации подлежат утверждению органом, отвечающим за реализацию и обеспечение соблюдения политики аккредитации пользователей СКР (например, ICANN, многосторонней комиссией), и периодическому пересмотру.
63.	Любая организация, являющаяся органом аккредитации пользователей СКР, должна заключить с ICANN и/или поставщиком СКР договор на выполнение таких процедур аккредитации в соответствии с согласованными руководящими принципами и создать систему, обеспечивающую правильное ведение дел, подотчетность, безопасность, справедливый доступ и соблюдение применимого законодательства.
64.	Органы аккредитации могут взять на себя одну или обе следующие обязанности. • Орган аккредитации пользователей СКР может создать сообщество пользователей и взять на себя управление этим сообществом, в том числе определение критериев членства, установление требований к получению учетных данных, а также формулирование и обеспечение соблюдения своих собственных условий и положений для членов сообщества. • Оператор аккредитации пользователей СКР может предлагать органам аккредитации платформу, обеспечивающую выполнение таких функций, как создание учетной записи пользователя, выдача, приостановка действия и аннулирование учетных данных, управление учетной записью пользователя в течение всего жизненного цикла и выполнение сопутствующих процедур, таких как разрешение споров и обеспечение соблюдения условий и положений. Конкретный орган аккредитации может, но не обязан, взять на себя обе задачи.

№ п/п	Принципы аккредитации пользователей СКР
65.	Органы аккредитации, желающие участвовать в обработке запросов к СКР на получение данных от имени своих членов, могут сделать это двумя способами: • Орган аккредитации может предоставлять доступ к СКР по доверенности через собственную систему проверки подлинности и брать на себя всю ответственность за правильность использования. Хотя в случае злоупотреблений ответственность будет нести орган аккредитации, проверка подлинности запросов, направляемых через органы аккредитации подобным образом по доверенности, должна осуществляться таким способом, который позволяет отследить в случае жалобы на злоупотребления доступ на уровне отдельного пользователя. • Орган аккредитации может предоставлять доступ к СКР по доверенности через собственную систему проверки подлинности, но при этом просто пересылать заверенные запросы в СКР. Запросы, направляемые через орган аккредитации подобным образом, должны однозначно идентифицировать пользователя СКР, который отвечает за правильность использования и в случае злоупотреблений будет лично привлечен к ответственности.
66.	Как было указано в разделе IV(b) «Принцип № 50», СКР должна предоставлять аккредитованным инициаторам запросов несколько способов доступа в режиме реального времени. Проверять подлинность запросов может соответствующий оператор аккредитации, а учетные данные СКР, выданные во время аккредитации, должны быть пригодны для использования со всеми установленными способами доступа.[16]
67.	Можно определить передовые практические методы управления учетными данными; необходимо, чтобы органы аккредитации придерживались этих передовых методов.
68.	Для доступа с проверкой подлинности СКР обязана требовать ввода индивидуальных учетных данных.
69.	Доступ к СКР с проверкой подлинности не должен быть транзитивным (то есть прошедший проверку подлинности пользователь СКР не должен передавать защищенные данные другим лицам за рамками своей аккредитации).

[16] На этапе реализации должны быть определены интерфейсы проверки подлинности. Например, для некоторых способов ввода учетных данных в СКР может использоваться стандартная система, такая как язык разметки, предусматривающий защиту данных (SAML), чтобы обеспечить выполнение проверки подлинности оператором аккредитации, выдавшим эти учетные данные.

№ п/п	Принципы аккредитации пользователей СКР
70.	Необходимо создать и обеспечить соблюдение процедуры ответственного раскрытия защищенных данных для выполнения первоначальной цели, ради которой они запрашивались. (Например, обеспечение возможности расследования нарушения прав на товарный знак владельцем ИС для подачи жалобы в рамках ЕПРД, разрешение пользователю из службы безопасности провести расследование возможной криминальной деятельности для уведомления правоохранительных органов.)
71.	Организация, стремящаяся получить доступ к данным СКР, может подать заявку на аккредитацию пользователя СКР и обеспечить охват всех людей, использующих СКР, этой единственной аккредитацией.[17] Каждая такая организация несет ответственность за управление аккредитованным доступом внутри своей организации. Неправильное использование системы членами организации, являющейся аккредитованным пользователем СКР, приведет к наложению санкций на организацию в целом.
72.	У одного пользователя СКР, выполняющего разные функции, может быть несколько учетных данных для доступа к сведениям разного типа для различных целей. Однако с точки зрения удобства для пользователя крайне желательно предоставлять единые учетные данные каждому пользователю СКР, которые можно было бы использовать для разных целей при условии, что каждая заявленная цель доступа соответствует указанным в разделе IV(b).
73.	Необходимо использовать аудиторские проверки и анализ данных для выявления злоупотреблений при использовании системы и учетных данных для доступа.
74.	Необходимо определить процедуру опротестования, позволяющую пользователям СКР опровергнуть обвинения в злоупотреблениях и снова активировать/восстановить свои учетные данные для доступа к СКР.
75.	Каждый владелец регистрации должен получить учетные данные, чтобы он мог проверить собственную контактную информацию, хранящуюся в СКР в связи с доменными именами, которые зарегистрированы с использованием этой информации. (См. раздел III, цель «Управление доменным именем».)

[17] Организация отвечает за обеспечение целостности любых учетных данных, выданных ей для доступа к СКР.

№ п/п	Принципы аккредитации пользователей СКР
76.	Необходимо ввести процедуру добавления дополнительных органов аккредитации пользователей СКР, которая либо дополняет существующие процедуры, либо предлагает новые, инновационные способы аккредитации пользователей для разрешенных целей в СКР. Такие органы аккредитации пользователей СКР должны отвечать минимальным требованиям, которые описаны в перечисленных здесь принципах.

г. Сводная информация о ключевых преимуществах в плане подотчетности

Включение аккредитации доступа к защищенным элементам данных в качестве неотъемлемой части СКР следующего поколения улучшит подотчетность за счет требования ко всем лицам, желающим получить доступ к более конфиденциальным данным, идентифицировать себя и сообщить о своей цели получения данных. В частности, к преимуществам, которые станут результатом внедрения рекомендуемых ЭРГ элементов данных и принципов доступа, относятся следующие.

- Введение парадигмы сбора и раскрытия данных на основе целей для содействия подотчетности субъектов, использующих регистрационные данные для разрешенных целей.
- Предоставление системы, обеспечивающей соблюдение законов о защите данных в различных юрисдикциях.
- Внедрение способа обеспечения подотчетности людей, получающих доступ к данным для различных целей. Это дополнительно поддерживает выполнение требований по защите данных/конфиденциальности в различных юрисдикциях и гарантирует равновесное распределение подотчетности между теми, кто обязан предоставлять точные данные, и теми, кто использует их для одобренных целей. Это устраняет принципиальное неравноправие в существующей системе WHOIS, где инициаторы запросов не несут никакой ответственности при получении доступа и использовании контактных данных.
- Обеспечение более четкого понимания владельцами регистраций и контактными лицами целей сбора регистрационных данных и предоставление им большей свободы принятия решений относительно того, какая личная информация будет общедоступной или защищенной.

- Удовлетворение всеобщей потребности в регистрационных данных благодаря основному набору общедоступных данных, наряду с сокращением количества данных, которые являются общедоступными по умолчанию, и проверкой подлинности лиц, получающих доступ к защищенным данным.
- Повышение точности данных вследствие защиты конфиденциальных элементов данных от публичного раскрытия, что повышает вероятность предоставления владельцами регистраций и ЦКЛ более точных данных. За исключением случаев злоумышленного использования, когда данные защищены от открытого опубликования, субъекты данных часто предоставляют более точные сведения, чтобы извлечь из этого пользу, поскольку принципиальный предполагаемый риск снижается.
- Улучшение общей отказоустойчивости и эффективности связи для пользователей СКР и владельцев регистраций за счет внедрения новых необязательных элементов данных с целью содействия установлению связи с помощью новых или альтернативных способов коммуникации.
- Поддержка обратных запросов и запросов WhoWas через центральный портал, позволяющая аккредитованным пользователям СКР выполнять поиск среди всех регистраций рДВУ только для разрешенных целей.
- Создание расширенных возможностей доступа для улучшения общей эффективности «системы».
- Предоставление доступа, как без проверки подлинности к общедоступным данным, так и с проверкой подлинности к защищенным данным, с целью устранения неразберихи в плане возможностей доступа, уровней обслуживания и форматов в сегодняшних ответах на запросы к WHOIS рДВУ, и обеспечения удобной реализации автоматизированных запросов к СКР с использованием единого стандарта.
- Предоставление качественных услуг и поддающегося контролю доступа, обеспечение возможности отказаться от разнообразных мер противодействия злоупотреблениям, распределенным по всей экосистеме.

Чтобы воспользоваться всеми указанными преимуществами, крайне важно будет обучить пользователей СКР тому, какие цели и варианты использования полученных из СКР данных являются разрешенными и целесообразными. При поиске органов аккредитации, желающих взять на себя ответственность за выдачу членам своих сообществ разрешений на доступ к СКР, могут возникнуть трудности. Первоначально, пользователи могут прийти в замешательство, пытаясь определить

надлежащий орган аккредитации, особенно те пользователи, которые взаимодействуют с СКР для нескольких целей. Для автоматизированных запросов СКР также потребуются средства обновления. Однако эти первоначальные инвестиции, которые необходимы для внедрения доступа на основе целей, заложат надежный фундамент обеспечения подотчетности пользователей СКР и ответственного использования регистрационных данных.

V. Улучшение качества данных

ЭРГ рекомендует повысить надежность проверки представленных владельцами регистраций данных, которые предусмотрены в сегодняшней системе WHOIS или с учетом ее возможной модернизации благодаря широкому внедрению CAP 2013. Во-первых, предоставление ЦКЛ владельцами регистраций должно привести к существенным улучшениям доступности надлежащих контактных лиц для различных целей и стимулировать владельцев регистраций к предоставлению точной информации о лицах, выполняющих данные роли. Во-вторых, при использовании регулируемого доступа к более конфиденциальным элементам данных у владельцев регистраций будет меньше побудительных причин предоставлять неточные данные и большая ответственность за обеспечение точности данных.

Чтобы достичь этих целей, ЭРГ рекомендует два смежных, но независимых улучшения:

- СКР должна применять стандартную процедуру подтверждения всех регистрационных данных рДВУ. Помимо периодических проверок, данные должны подтверждаться во время их сбора с возможностью предварительной проверки блоков контактных данных для неоднократного использования при регистрации нескольких доменных имен.
- В состав экосистемы СКР должен входить предварительно проверенный каталог контактных данных, принципиально независимый от каталога доменных имен, для содействия качеству и возможности неоднократного использования элементов данных, используемых для связи с владельцами регистраций и людьми или организациями, которые могут быть назначены владельцами регистраций в качестве ЦКЛ для различных целей, связанных с регистрацией доменных имен, и для ограничения мошеннического использования личных данных.

Принципы и процедуры, детализирующие данные рекомендации, подробно изложены ниже. Для получения максимальной пользы ЭРГ рекомендует оба улучшения, однако отмечает, что создать каталог контактных данных можно без усиления проверки, и наоборот.

a. Принципы обеспечения точности и подтверждения данных

Предварительная проверка сведений о владельце регистрации и другой контактной информации желательна, чтобы:

- повысить точность контактной информации путем использования предварительного подтверждения, благодаря проверке данных перед их использованием для нового доменного имени и содействию согласованности данных всех регистраций (сокращает количество ошибок и мошенничества);
- избежать необходимости проверки контактных данных владельца регистрации или иного ЦКЛ при каждой регистрации этим владельцем нового доменного имени, выполнив проверку один раз, а затем неоднократно используя этот блок контактных данных для регистрации нескольких доменов (упрощает процедуру и снижает рабочую нагрузку); и
- избежать задержки при обработке регистрации доменов, поскольку проверка данных должна выполняться во время регистрации.

Многие поставщики услуг, законные представители и другие третьи лица часто являются основными точками контакта, выполняющими нескольких функций (например, техническую, выставления счетов, борьбы со злоупотреблениями, ведения судебных процессов) для доменов, зарегистрированных широким спектром владельцев регистраций (часто для сотен или сотен тысяч доменов).

Чтобы намного повысить точность данных и удобство использования этих контактных лиц в таком многообразном пространстве, желательно предусмотреть простые механизмы использования таких контактных лиц множеством владельцев регистраций; например, предоставление хостинговой компанией уникального идентификатора своего операционного сетевого центра (NOC) для связи по «техническим» вопросам и вопросам «злоупотреблений», которые касаются доменов, контролируемых клиентами данной компании. Кроме того, когда такой организации необходимо обновить свою контактную информацию, чтобы отразить в ней новый адрес/номер телефона или операции слияния/приобретения, было бы удобно обновлять такую информацию в одном месте, а затем отражать ее во всех доменах, связанных с этим множеством контактных данных (обозначенным уникальным идентификатором).

На следующем рисунке проиллюстрирована парадигма, в которой целевые контактные лица (ЦКЛ) могут создаваться, связываться с уникальными идентификаторами (идентификаторы ЦКЛ), а затем неоднократно использоваться при регистрации нескольких доменных имен. Как подробно описано в разделе III, ЦКЛ не обязательно означает физическое лицо, а скорее представляет собой опубликованную точку контакта, созданную владельцами контактных данных специально для возможности связи по вопросам, относящимися к DNS.

Обновления ИД ЦК №3,
автоматически отраженные в регистрационных
данных для доменных имен A и B

№ п/п	Принципы использования идентификаторов контактных лиц и соответствующих данных
77.	Должна быть возможность раздельного управления контактными лицами и доменами, что обеспечит мобильность и подотчетность контактов независимо от доменных имен и под контролем реальных физических или юридических лиц, перечисленных в составе таких контактных данных.
78.	Управление контактными лицами необходимо осуществлять с привлечением проверяющих, которые управляют базами контактных данных, внедряют режимы проверки и хранят информацию об уровне действительности контакта и его элементов данных (которые доступны через СКР).[18]

[18] ПРИМЕЧАНИЕ: Регистраторы могут и, предположительно, станут аккредитованными проверяющими, которые оказывают услуги подтверждения контактных данных, связанных с регистрируемыми ими доменными именами.

№ п/п	Принципы использования идентификаторов контактных лиц и соответствующих данных
79.	Зарегистрированные домены могут быть связаны с идентификаторами контактных лиц, которые были назначены соответствующими владельцами регистраций и утверждены этими указанными контактными лицами для различных целей, связанных с доменным именем.
80.	В состав сведений о таких контактных лицах должны входить достоверные обязательные элементы данных. Потребуются политики и процедуры надзора для управления указанными процессами с целью обеспечения того, что идентификаторы контактных лиц не используются без одобрения со стороны контактного лица и отвечают минимальным нормам.
81.	Управление изменениями и авторизацией использования контактных данных осуществляет владелец контактных данных, действия которого влияют на все домены, связанные с этим контактным лицом. Для поддержки этой новой парадигмы необходимо разработать процедуры и политики, обеспечивающие точность, достоверность и своевременность внесения желательных изменений без обременения ЦКЛ или владельцев регистраций.
82.	У каждого отдельного блока контактных данных должен быть свой идентификатор контактного лица, который однозначно идентифицирует как проверяющего, так и владельца контактных данных, чтобы обеспечить возможность получения и обновления соответствующих контактных данных. Этот идентификатор контактного лица должен публиковаться в любой системе публичного отображения данных СКР.

б. Процедура предварительной проверки

Для удовлетворения указанных потребностей рекомендуется следующая процедура предварительной проверки:

а) Каждый кандидат отправляет контактные данные через выбранного по своему усмотрению проверяющего (например, регистратора, реестр, аккредитованного стороннего поставщика услуг управления контактными данными).

б) Проверяющий выполняет синтаксическую и функциональную проверку (согласно SAC-058).

в) **ДОПОЛНИТЕЛЬНО**: Проверяющие могут выполнять подтверждение личности, используя для этого почтовые организации, управляющих нДВУ, телефонные компании, налоговые инспекции и т. д. *Следует обратить внимание, что в статусе контактных лиц, прошедших дополнительную процедуру подтверждения личности, можно указать на это, чтобы повысить доверие пользователей, которое способствует электронной торговле. Также следует обратить внимание на то, что такие дополнительные услуги,*

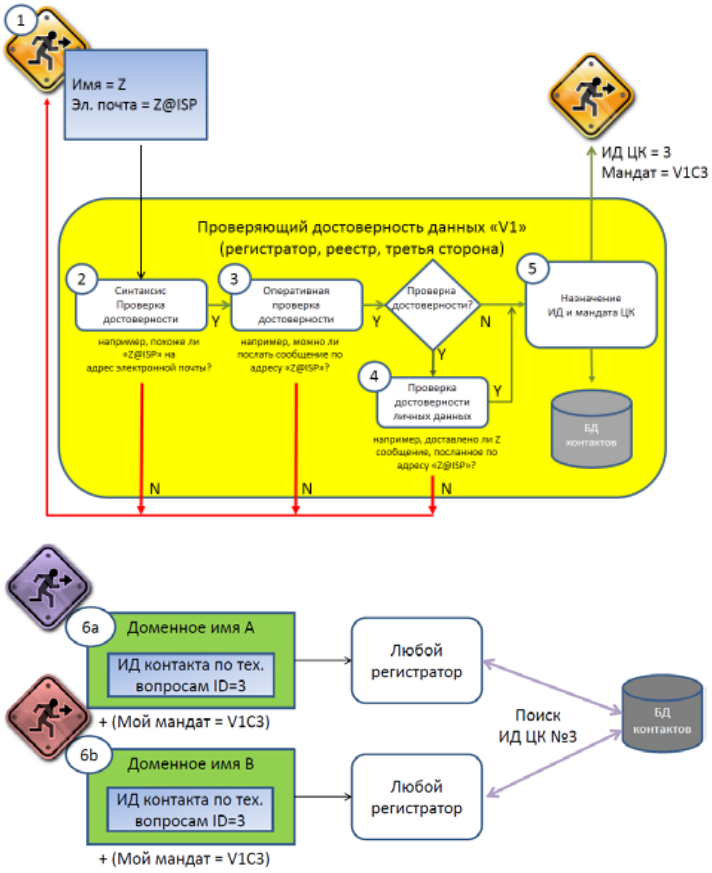
скорее всего, приведут к добавочным расходам для тех субъектов, которые будут запрашивать этот дополнительный уровень подтверждения.

г) После успешной синтаксической проверки и необходимой функциональной проверки проверяющий присваивает блоку контактных данных (контактному лицу) идентификатор, однозначно определяющий как проверяющего, так и контактное лицо, и в дальнейшем позволяющий получать и обновлять данные.

д) Проверяющий хранит контактные данные в собственной базе данных, выдает учетные данные (в соответствующих случаях, чтобы обеспечить возможность будущего обновления контактных сведений) и пересылает уникальный идентификатор заявителю (с этого момента называемому владельцем контактных данных).

е) Владелец контактных данных предоставляет этот идентификатор контактного лица владельцам регистраций, которые затем могут использовать этот уникальный идентификатор при регистрации доменных имен у любого регистратора в качестве идентификатора контактного лица для назначенных целевых контактных лиц (то есть ЦКЛ). *Как определено в разделе III, должна использоваться процедура авторизации, чтобы обеспечить согласие владельца регистрации и назначенного контактного лица относительно целей, которые это ЦКЛ готово выполнять для каждого доменного имени.*

ж) Проверенные идентификаторы контактных лиц могут назначаться в качестве ЦКЛ для доменного имени (например, владелец регистрации, контактное лицо по техническим вопросам, по административным вопросам, по коммерческим вопросам, по вопросам злоупотреблений, по правовым вопросам, поставщик услуг сохранения конфиденциальности/регистрации через доверенных лиц) в соответствии с принципами для целевых контактных лиц, которые определены в разделе III(e).



Следует обратить внимание, что каждый проверяющий обслуживает свою собственную базу контактных данных. Эти данные также должны быть предоставлены в СКР, однако данный механизм зависит от модели СКР, как описано в разделе VII. Например, в синхронизированной модели добавленные и обновленные контактные данные могут передаваться в СКР по протоколу EPP. В интегрированной модели контактные данные могут извлекаться СКР в режиме реального времени по протоколу RDAP.

в. Процедура обеспечения точности, аудита и исправления нарушений

Рекомендуется использовать следующие процедуры для постоянного обеспечения точности регистрационных данных и исправления неточностей в регистрационных данных:

а) **Самостоятельное исправление**: Владелец контактных данных использует проверяющего для исправления/обновления своих данных при помощи ранее выданных учетных данных. Информация автоматически распространяется среди всех доменов, использующих это контактное лицо (что обозначено соответствующим идентификатором контактного лица).

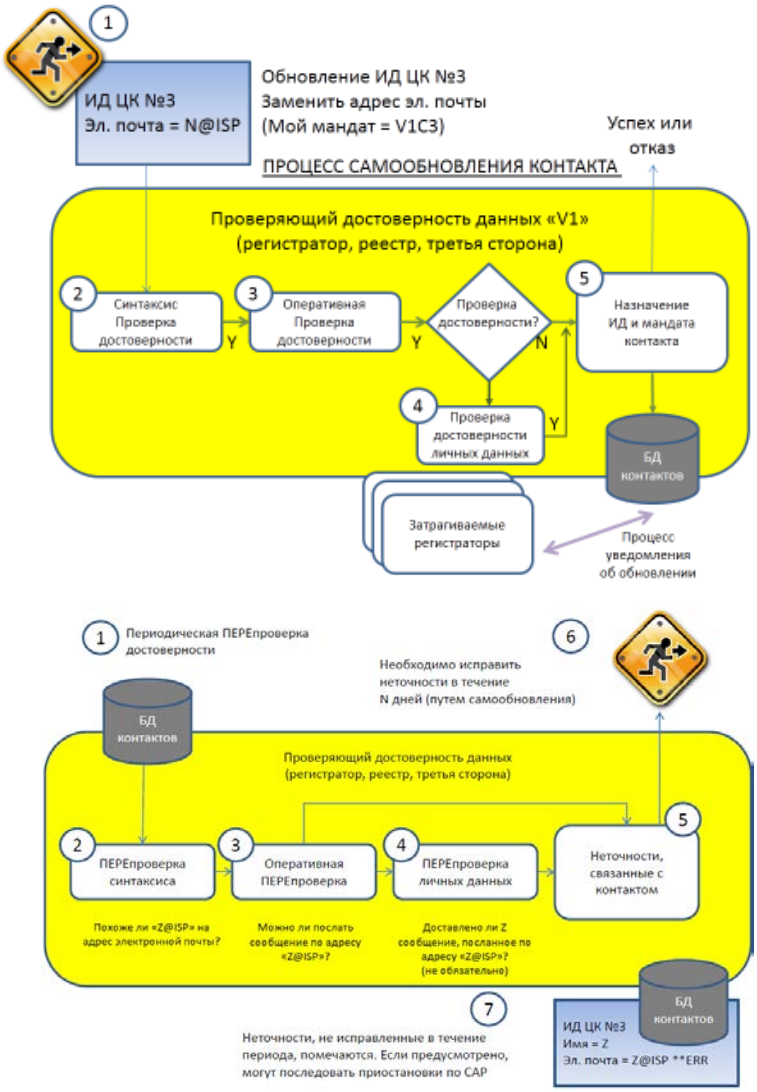
б) **Контролируемая процедура**: Проверяющие проводят периодические функциональные проверки и необязательные подтверждения личности для совокупностей контактных данных, управление которыми осуществляется с использованием их услуг. *Примечание: такие процедуры проверок не должны быть слишком обременительными, но могут отражаться в публикуемом состоянии любого контактного лица (например, «Контакт функционирует по состоянию на 1 января 2016 года»).*

в) Проверяющие сообщают владельцу контактных данных обо всех обнаруженных неточных данных и дают владельцу контактных данных определенный срок (например, 14 дней) для устранения ошибки. Могут быть проинформированы владельцы регистраций, реестры и регистраторы любых затрагиваемых доменов. Владелец контактных данных использует выбранного ранее проверяющего для исправления ошибки при помощи ранее выданных учетных данных.

г) Если регистрационные данные остаются неточными по истечении срока, эти данные помечаются как некорректные. Если помеченные данные являются обязательными для любого ЦКЛ, которое в данный момент ссылается на этот идентификатор контактного лица, соответствующие домены подвергаются процедуре исправления нарушений, которая предусматривает уведомление владельца регистрации о некорректности данных и предоставление ему возможности устранить ошибку в отведенный согласно положениям САР срок. Если ситуация не будет исправлена, это может привести к санкциям для доменного имени, в число которых может входить приостановка действия или удаление доменного имени, в соответствии с применимым САР.

д) После того как помеченные данные будут заменены действительными данными, любые санкции с затрагиваемых доменов снимаются.

е) Если сообщения о неточности данных будут направлены в отдел соблюдения договорных обязательств ICANN, проверяющий получит уведомление о необходимости повторить синтаксическую и функциональную проверку. Если повторная проверка пройдет успешно, сообщившая о неточности сторона имеет право принять другие меры, сообразно своей ситуации (например, подать жалобу ЕПРД или направить запрос на раскрытие данных). Если повторная проверка закончится неудачно, владельцев регистраций всех доменных имен, использующих этот некорректный идентификатор контактного лица, необходимо уведомить об этом и выполнить стандартную процедуру исправления нарушений, которая описана выше.



г. Организационная структура для идентификаторов контактных лиц

Для управления идентификаторами контактных лиц и их связи с регистрационными данными рекомендуется использовать следующую схему:

а) Идентификаторы контактных лиц должны быть уникальными среди всей совокупности проверяющих, чтобы обеспечить переносимость идентификаторов и однозначное сопоставление доменных имен и необходимой справочной информации.

б) Идентификаторы контактных лиц, в которых указано как контактное лицо, так и проверяющий, должны быть связаны с отдельными блоками контактных данных для обеспечения возможности извлечения и обновления информации. Разъяснение: идентификатор контактного лица сопоставляется с

совокупностью контактных данных, которая пригодна для установления связи с указанными контактными лицами доменного имени. Сведения, для которых это требование не выполнено, функционально бесполезны.

в) Идентификаторы контактных лиц должны выдаваться аккредитованными проверяющими. Организация может подать заявку, чтобы стать проверяющим, с учетом критериев, аналогичных тем, которые сейчас используются для аккредитации регистраторов. Аккредитованными проверяющими могут становиться регистраторы, реестры и сторонние поставщики услуг проверки. Обоснование: проверяющий — необходимый для создания базы контактных данных функциональный орган. Глубина проверки может меняться в зависимости от контактного лица, однако эту процедуру необходимо сделать единообразной для всех проверяющих, чтобы обеспечить точность и подотчетность перед владельцами регистраций доменных имен и назначаемыми контактными лицами.

г) Чтобы быть связанным с доменным именем, владельцу регистрации или назначенному ЦКЛ необходимо получить идентификатор контактного лица.

д) Идентификаторы контактных лиц могут назначаться для нескольких функций в одном или множестве доменов. Например, конкретный идентификатор ЦКЛ может одновременно использоваться как идентификатор владельца регистрации одного домена и идентификатор контактного лица по техническим и административным вопросам других доменов.

е) Контактных лиц можно создавать и изменять в любое время, в том числе на одном из этапов процедуры регистрации домена.

д. Взаимодействие с проверяющими

ЭРГ рекомендует использовать для взаимодействия проверяющих с владельцами контактных данных (то есть сторонами, которые успешно создают проверенные и допускающие возможность неоднократного использования блоки контактных данных) следующие принципы.

№ п/п	Принципы взаимодействия между владельцами контактных данных и проверяющими
83.	Для любого отдельно взятого идентификатора контактных данных владелец контактных данных имеет право выбрать любого проверяющего[19].
84.	Должны быть разработаны политики надзора и обеспечения подотчетности, связанные с управлением идентификаторами контактных лиц.
85.	Владельцы контактных данных должны иметь возможность изменения контактных данных, которые связаны с идентификатором контактного лица, через выдавшего этот идентификатор проверяющего.
86.	Проверяющие должны осуществлять проверку подлинности владельцев контактных данных, чтобы предотвратить несанкционированное изменение информации, связанной с идентификатором контактного лица.
87.	Проверяющие могут предлагать проверку подлинности владельца контактных данных на нескольких уровнях, от базовой идентификации по личному номеру до двухфакторной проверки подлинности. Владельцы контактных данных должны иметь возможность выбора поставщиков, исходя из своих предположений относительно соотношения издержек и выгод в плане удобства использования, безопасности, расходов и других логичных коммерческих факторов.
88.	Проверяющие обязаны публиковать свои политики проверки подлинности таким образом, который может использоваться для управления репутацией в мировом масштабе. Это будет стимулировать улучшение точности и ответственности для включенных в список контактных данных.
89.	Проверяющие обязаны иметь возможность проверки представленных контактных данных на родном языке владельца контактных данных. Это должно повысить точность данных, представленных на родном языке, и поддержать масштабируемость системы регистрации доменных имен в многоязычной среде. Например, регистраторы могли бы работать с проверяющими в различных регионах, предоставляя расширенные услуги проверки большому количеству владельцев регистраций и назначаемых контактных лиц без необходимости инвестиций в дорогостоящие средства подтверждения данных на тех языках, которыми не владеют их сотрудники.

[19] Согласно принципу № 88, идентификаторы контактных лиц определяют и проверяющего, и владельца контактных данных. Это следует реализовать таким способом, который позволяет переносить идентификаторы контактных лиц от одного проверяющего к другому.

e. Принципы проверки контактных данных

Контактные данные могут проверяться на трех различных уровнях: синтаксическом, функциональном и идентификационном, в соответствии с документом SAC 058. ЭРГ рекомендует следующие принципы проверки на разных уровнях.

№ п/п	Принципы проверки контактных данных
90.	Все элементы контактных данных, связанные с идентификатором контактного лица, должны проверяться на синтаксическом уровне. Это является проверкой базового уровня, которую обязана выполнять любая организация, работающая в данной отрасли.
91.	Все обязательные элементы контактных данных, связанные с идентификатором контактного лица для конкретной цели, должны пройти функциональную проверку,[20] прежде чем этот идентификатор контактного лица можно будет включить в состав регистрационных данных доменного имени для этой цели.
92.	Владелец контактных данных может по своему желанию стремиться к повышению уровня проверки (например, к выполнению необязательной проверки личности), взяв на себя соответствующие расходы ради ожидаемых выгод (например, повышения доверия потребителей к доменным именам, которые зарегистрированы субъектами, прошедшими проверку личности)[21].
93.	Учитывая расходы, связанные с проведением необязательной проверки личности, желательно иметь низкозатратный механизм прохождения такой проверки неимущими владельцами контактных данных.
94.	Чтобы сохранить связи и обеспечить возможность процесса исправления, идентификатор контактного лица может иметь состояние «некорректный» и оставаться в системе.
95.	Состояние проверки идентификатора контактного лица должно отслеживаться и надлежащим образом публиковаться при получении доступа к информации СКР, наряду с временем определения последнего состояния проверки.

[20] Чтобы ознакомиться с возможными способами реализации функциональной проверки и существующей практикой нДВУ, см. документы SAC 058 и *Сводная информация о результатах исследования проверки/подтверждения данных WHOIS в нДВУ*.

[21] К примеру, необязательная проверка личности могла бы стать оплачиваемым отдельно дополнением или войти в составов пакетов регистрации доменных имен, или предлагаться как поощрительное вознаграждение оптовых клиентов. Примеры коммерческих услуг, в рамках которых выполняется такая проверка, см. в документе *Запрос информации по подтверждению контактных данных и системам проверки*.

№ п/п	Принципы проверки контактных данных
96.	Третьи лица имеют право направлять сообщения о неточностях и оспаривать состояние проверки идентификатора контактного лица, как описано в разделе V(c), запуская стандартную процедуру устранения нарушений, которая может привести к присвоению идентификатору контактного лица метки «некорректный» и к дальнейшим последствиям для доменных имен, использующих этот идентификатор контактного лица как ЦКЛ.
97.	У активных доменов обязательный контакт не может иметь состояние «некорректный», и такая ситуация потребует исправления. Однако соответствующая схема может быть определена в другом документе.
98.	Должна выполняться минимальная перекрестная проверка полей для всех элементов данных, связанных с идентификаторами контактных лиц, к которым такая перекрестная проверка полей применима (например, для физического адреса).
99.	Соответствующий проверяющий должен регулярно выполнять перепроверку контактных данных, чтобы обеспечить сохранение их точности на заявленном уровне.
100.	Если владелец контактных данных предоставляет необязательные элементы данных, они должны пройти как минимум синтаксическую проверку. Необязательные элементы данных не будут проверяться на уровне, превышающем синтаксическую проверку, если только владелец контактных данных не направит соответствующий запрос и, предположительно, оплатит все расходы, связанные с такой проверкой.
101.	Достигнутый помимо синтаксической проверки уровень проверки элементов данных, которые могут быть подвергнуты функциональной проверке или (необязательной) проверке личности, должен быть зарегистрирован и сохранен проверяющим. Например, такие элементы как электронная почта, телефон и адрес могут быть проверены на функциональном уровне, в то время как имя физического лица или наименование организации не могут быть проверены функционально, но могут в необязательном порядке пройти проверку личности.
102.	Кроме того, проверяющий обязан определить и опубликовать как элемент данных СКР общее состояние проверки, достигнутое каждым идентификатором контактного лица. Например, если ВСЕ обязательные элементы данных, которые можно проверить на функциональном уровне, прошли такую проверку, общим состоянием проверки контактного лица может быть «функционально проверено». Если ЛЮБОЙ обязательный

№ п/п	Принципы проверки контактных данных
	элемент данных, которые можно проверить на функциональном уровне, не прошел такую проверку, общее состояние проверки контактного лица должно быть снижено до уровня «синтаксически проверено». Если ВСЕ обязательные элементы данных, которые можно проверить на уровне идентификации личности, прошли такую необязательную проверку, общее состояние проверки контактного лица можно повысить до уровня «личность проверена». Чтобы способствовать точности и эффективности связи, это общее состояние проверки должно быть доступно пользователям СКР как отдельный новый консолидированный элемент данных контактного лица.[22]
103.	Для любого прошедшего проверку элемента данных проверяющий также должен зарегистрировать и сохранить метку времени этой проверки.
104.	Метка времени последнего изменения общего состояния проверки всего идентификатора контактного лица также должна быть определена проверяющим и опубликована как новый элемент данных СКР для этого контактного лица.

ж. Право на уникальность контактных данных

Чтобы препятствовать выдаче себя за другое лицо, клевете и злоупотреблениям, владелец контактных данных вправе указать, что его контактные данные уникальны и не должны использоваться другими лицами, претендующими на статус владельцев контактных данных.

а) К уникальным могут относиться многие сведения из набора контактных данных, в частности, адрес электронной почты и номер телефона. Гарантировать уникальность адресов и имен трудно или невозможно.

б) Если владелец контактных данных направляет запрос на регистрацию уникальности, другим проверяющим необходим механизм сравнения указанного в запросе множества контактных данных этого владельца, чтобы новые претенденты на регистрацию идентификатора контактного лица

[22] ЭРГ также рассмотрела возможность опубликования элементов данных СКР для отражения индивидуального состояния проверки каждого отдельного элемента контактных данных (например, состояние адреса электронной почты ЦКЛ = функционально проверено, состояние имени ЦКЛ = личность проверена). Для опубликования состояний проверки с такой степенью детализации потребуются существенные изменения протокола, элементов данных и клиентского приложения/ГИП, поэтому такая рекомендация не была дана в настоящее время, но, возможно, заслуживает дальнейшего изучения.

(или существующие владельцы контактных данных при изменении своих сведений) не смогли использовать уникальные защищенные данные.[23]

в) Любые данные, обозначенные как уникальные, должны быть проверены на уровне идентичности личности, чтобы препятствовать выдаче себя за другое лицо и атакам типа «отказ в обслуживании» (когда имеющее законные права контактное лицо не может использовать свои достоверные данные).

з. Сводная информация о ключевых преимуществах качества данных

Внедрение систем управления идентификаторами контактных лиц и проверка в качестве неотъемлемой части СКР следующего поколения повысит качество данных, сделав более сложным для владельцев регистрации включение ложных данных в СКР и снизив масштабы мошенничества и хищения персональных данных. В частности, к преимуществам внедрения рекомендуемых ЭРГ принципов обеспечения точности и проверки данных, относятся следующие.

- Расширение возможностей физических лиц и организаций по управлению контактными данными и их сохранению, независимо от места использования этих данных в экосистеме доменных имен.
- Создание больших трудностей для злоумышленников, стремящихся получить доменные имена, благодаря необходимости проверки всех контактных лиц на минимальном уровне при регистрации или обновлении доменных имен. Требования по аккредитации проверяющих должны обеспечить выявление и наказание тех проверяющих, которые не соответствуют функциональным стандартам, совершают мошеннические действия и небрежно относятся к своим обязанностям. При выявлении злоумышленника, владеющего одним из зарегистрированных доменных имен, благодаря общему для всех доменов ЦКЛ можно обнаружить остальные принадлежащие ему домены и исправить ситуацию.
- Повышение согласованности данных у нескольких доменных имен, зарегистрированных конкретным владельцем. Хотя могут возникать некоторые предварительные расходы на проверку конкретного контакта, введение единого переносимого идентификатора контактного лица позволяет слаженно осуществлять дополнительные регистрации и должно существенно сократить будущие расходы на обслуживание для многих владельцев регистраций.

[23] Проверку уникальности относительно просто выполнить в синхронизированной модели СКР, однако в интегрированной модели СКР она может быть более затруднительной.

- Улучшение возможности обнаружения недействительной контактной информации с течением времени и применение исправлений ко всему множеству доменов, использующих эту контактную информацию. Требования к проверяющим относительно проведения периодических проверок или проверок после любых обновлений выдвигают на передний план проблемы устаревшей контактной информации и позволяют в рамках одного изменения применить обновленные сведения для всех затрагиваемых доменных имен.
- Улучшения в плане затрат и эффективности для всей экосистемы. Несмотря на усложнение общей системы регистрации, управление контактными данными можно отделить от управления регистрациями доменных имен, что позволит осуществлять широкомасштабные обновления доменов одновременно с возможностью локализации управления контактными данными.
- Появление у поставщиков услуг возможности беспроблемно обновлять свои контактные данные для тех доменов, где они являются целевыми контактными лицами, без необходимости обновления индивидуальных регистраций доменных имен. В ситуациях с множеством поставщиков это позволило бы без труда обновлять тысячи и даже миллионы доменных имен.
- Сокращение количества злоупотреблений путем выдачи себя в регистрационных данных за другое лицо благодаря дополнительной проверке личности. Хотя необязательная проверка личности, скорее всего, будет сопряжена с расходами для владельца контактных данных, который будет ее проходить, возможность защиты от злоупотреблений путем выдачи себя за другое лицо (хищения персональных данных), с которой ежедневно сталкиваются организации высокого ранга, крупные поставщики услуг или преследуемые с преступными намерениями физические лица будет оправдывать такие расходы.
- Отделение управления и проверки контактных данных от регистрации и управления доменными именами обеспечивает более точное сопоставление субъектов данных и принадлежащих им сведений, повышая удобство применения надлежащих законов о защите данных, поскольку проверяющие могут находиться в местной юрисдикции владельца контактных данных, независимо от местонахождения регистратора или реестра.
- Проверяющие могут предоставлять владельцам контактных данных и владельцам регистраций услуги на местном языке, повышая качество и точность данных и снижая, тем самым, расходы на проверку. Это позволило бы

регистраторам через распределенную совокупность проверяющих предлагать услуги на тех языках, на которых персонал регистратора не может без труда осуществлять поддержку или самостоятельную проверку данных.

VI. Правовые и договорные факторы

В своей работе ЭРГ руководствовалась некоторыми главными правовыми принципами:

Личные данные должны: • обрабатываться законным, справедливым и прозрачным по отношению к субъекту данных образом; • собираться для конкретных, очевидных и законных целей и не обрабатываться каким-либо способом, не совместимым с этими целями; • быть адекватными, уместными и ограниченными минимально необходимым объемом в соответствии с целями, для которых они обрабатываются, и • быть точными и актуальными, насколько этого требуют указанные цели.
Законная обработка, включая передачу и раскрытие, может быть основана — с учетом соответствующей юрисдикции — на следующих принципах: • согласие субъекта данных; • необходимость выполнения договора, одной из сторон которого является субъект данных, и • необходимость соблюдения своей правовой обязанности контролирующим лицом.
Необходимо обеспечить реализацию права субъекта данных на доступ к информации и права на исправление неточностей.

ЭРГ рекомендует рассмотреть эти и другие сопутствующие принципы, которые обычно включаются в законы о защите данных, при разработке окончательных политик и процедур реализации СКР. Кроме того, группа полностью признает, что в некоторых юрисдикциях права на неприкосновенность частной жизни распространяются на юридических лиц и организации в отношении свободы слова и свободы объединения. ЭРГ признает обе указанные отдельные группы прав, которые защищены раздельно и по-разному в разных странах мира.

На данной основе ЭРГ оценила варианты и затем сформулировала принципы СКР в отношении конфиденциальности и защиты данных, а также доступа право-охранительных органов. Эти принципы ЭРГ представлены в настоящем разделе и поддерживаются принципами соблюдения договорных обязательств, подотчетности и аудиторских проверок.

a. Принципы защиты данных

Сегодня практические методы применения действующего национального законодательства о защите частной жизни и потребителей неоднородны. Некоторые законы требуют, чтобы при экспорте данных физического лица за пределы его юрисдикции или юрисдикции обработчика данных, деятельность которого регулируется этим законом, применялись аналогичные или эквивалентные средства защиты данных. Европейская директива о защите данных 1995 года не разрешает передавать данные за пределы этой юрисдикции, если только местное законодательство не будет признано «надлежащим». Многие другие юрисдикции за пределами ЕС стремятся к более строгим положениям договоров, однако в любом случае большинство законов запрещает лицам, владеющим персональными данными, передавать их или раскрывать другим в отсутствие согласия, если только не будет гарантирована их защита. В этой точке передачи может возникнуть ответственность по претензиям. На данный момент ICANN решила этот вопрос, разрешив в CAP регистраторам отказаться от выполнения требования по депонированию данных, если они продемонстрируют, что на эти данные распространяются законы о защите данных, запрещающие депонирование. Это не единственное положение в экосистеме ICANN, которое создает риск для лиц, стремящихся соблюдать законы о защите данных, поэтому было предложено тщательно изучить существующее положение дел. Учитывая внимание, которое ЭРГ уделяла в своей работе подотчетности, требование нести ответственность за защиту данных было изучено.

Сегодня требования о том, чтобы получающая персональные данные организация гарантировала их надлежащую защиту, которая соответствует средствам защиты, предоставленным субъекту данных «дома», выполняются **в зависимости от конкретного случая**— от того, находится ли получающая данные организация в юрисдикции, где предусмотрена законодательная защита данных или аналогичная надлежащая защита. Это означает, что либо адекватность защиты обеспечивается законом, применимым к получающей данные организации, либо вводятся другие гарантии обеспечения законности передачи данных с точки зрения законодательства, применимого к субъекту данных.

Механизмы защиты данных

С учетом текущей ситуации, были изучены четыре варианта поэтапной защиты персональных данных во всей экосистеме СКР:

(0) не предпринимать никаких действий;

(1) внедрить механизмы, способствующие повседневному законному сбору и передаче данных;

(2) внедрить механизмы, нацеленные на гармонизацию защиты конфиденциальности и данных во всей экосистеме ICANN, чтобы создать «фундамент» защиты данных, устанавливающий признанные передовые практики в сфере политики сохранения конфиденциальности; и

(3) представить эту политику в виде совокупности «обязательных корпоративных правил».

Примечание: в тексте этого раздела употребляется термин «экосистема СКР», который относится ко всем участникам, перечисленным в разделе VIII(c) «Договорные отношения и соблюдение договоров» и в разделе VIII(d) «Подотчетность и аудит». Сюда относится ICANN (как зарегистрированная в США некоммерческая корпорация), все реестры и регистраторы рДВУ (каждый из которых функционирует как независимая корпорация, находящаяся во многих странах), а также все новые аккредитованные организации, предложенные ЭРГ в настоящем документе: поставщик СКР, проверяющие, органы утверждения защищенных учетных данных, органы аккредитации пользователей СКР, отдел обеспечения соблюдения договорных обязательств ICANN и любые другие организации, участвующие в обработке персональных данных.

Вариант (0): «не предпринимать никаких действий»

Результатом отказа от действий стала бы очень высокая сложность по причине сохранения риска несоблюдения законов о защите данных и необходимости изучения каждой регистрации для определения применимого законодательства. Для некоторых операторов, а именно реестров, это было бы сопряжено с существенными накладными расходами. Для регистраторов это могло бы стать причиной высоких расходов на текущий контроль адекватности защиты, которая требуется владельцам регистрации и реестрам. Это привело бы к росту потенциальной юридической неопределенности для всех сторон, в том числе ICANN и других заинтересованных сторон системы доменных имен. Увеличение

количества рДВУ и многообразия мест расположения реестров создает новые трудности, касающиеся применимого законодательства и юрисдикции для системы договорных отношений ICANN в плане неприкосновенности личной жизни владельцев регистраций и защиты потребителей. Беспорядок, неопределенность и разнородность практических методов потребовали бы от ICANN больших усилий по обеспечению соблюдения договорных обязательств и снижению потенциального риска. Эти трудности существуют независимо от вопроса СКР. После ввода в эксплуатацию более 1000 новых рДВУ, проблема станет еще более острой. Важнее всего то, что невозможно гарантировать согласованную защиту субъектов данных . В разработке концепции гармонизации, которая уменьшает риск, минимизирует нагрузку и снижает сложность заинтересованы все стороны.

Вариант (1): внедрить механизмы, способствующие повседневному законному сбору и передаче данных

Вторым рассмотренным вариантом является внедрение системы, которая будет оценивать соответствующее законодательство о защите конфиденциальности и данных и представлять его в виде перечня, чтобы заинтересованные стороны могли его применять, а физические лица — узнавать о том, где находятся их данные и какие законы на них распространяются. Этот перечень мог бы применяться СКР автоматически через «обработчик правил», как определено в следующем разделе. Если физическое лицо проживает в стране, где есть закон о защите данных и этот закон действует за пределами страны для персональных данных, переданных этим лицом другой стороне (в данном случае регистратору), этот закон может быть применен. Если регистратор находится в стране, чьи законы о защите данных распространяются на всех физических лиц (то есть не только на граждан этой страны), то этот закон может быть применен вне всякого сомнения. Рассматриваемыми для этой цели или в указанных пределах данными считаются только те, которые накоплены в СКР[24]. Кодирование данных о юрисдикциях, которые применяются в экосистеме, упростило бы жизнь затрагиваемых заинтересованных сторон, обеспечило бы соблюдение прав владельцев регистраций на защиту данных (в случае применимости) и снизило бы риск несоблюдения требований. Однако в юрисдикциях, где отсутствуют законы о защите данных, распространяющиеся на отрасль регистрации доменных имен, реестры или ICANN и ее механизмы обеспечения

[24] Это не обязательно упростило бы жизнь регистраторов, которые контролируют намного более конфиденциальные данные, например банковские реквизиты, информацию о кредитных картах, регистрационные записи о технической поддержке клиентов и т. п., которые не передаются в СКР, хотя «обработчик правил» был бы полезен в некоторых ситуациях, учитывая сложность будущей системы рДВУ.

соблюдения обязательств, этот сценарий обеспечивает небольшую защиту отдельных владельцев регистраций. Это могло бы привести к созданию многоуровневой системы прав на неприкосновенность личной жизни, в которой у некоторых владельцев регистраций не было бы никаких прав человека, в то время как у других были бы все права и основания для юридического надзора.

Вариант (2): внедрить механизмы, которые были бы нацелены на гармонизацию защиты данных во всей экосистеме СКР, чтобы создать «фундамент» защиты данных, определяющий признанные передовые практики в сфере политики сохранения конфиденциальности

Можно было бы подготовить положения договоров, устраняющие любые несоответствия в защите конфиденциальности (подробнее рассматривается в разделе, посвященном реализации), и в основе этих положений мог бы лежать общепризнанный набор средств защиты конфиденциальности, который сформировал бы основу политики ICANN в отношении защиты конфиденциальности. Эта политика могла бы быть краткой, содержащей перечень соответствующих статей в приложении. Это позволило бы беспрепятственно передавать данные между участниками экосистемы СКР, обеспечив такой уровень защиты данных, который был бы достаточно высок для предотвращения возражений по соображениям неприкосновенности личной жизни, защиты данных и прав потребителей.

Механизмы, способствующие законному сбору и передаче данных во всей экосистеме СКР, могли бы принимать разные формы, но все они должны быть основаны на последовательной политике защиты данных в СКР. ICANN обеспечивала бы соблюдение этой политики всеми заинтересованными сторонами через положения договоров, как она это делает для большинства других политик.

Вариант (3): на основе пункта (2) выше, эту политику можно было бы представить в виде совокупности «обязательных корпоративных правил», признаваемых законами о защите конфиденциальности/данных стран АТЭС и ЕС

Это вариант упростил бы операции передачи данных между 28 странами Европейского Союза, поскольку он обеспечивает установление адекватной для входящих в ЕС государств защиты данных и устраняет узкоспециализированный характер решений по защите данных, обусловленных потоками данных в экосистеме СКР. Хотя для реализации этого варианта может потребоваться больше времени, он мог бы снизить риск несоблюдения требований и обеспечить лучшую защиту. Это также обеспечило бы независимый надзор над политикой защиты конфиденциальности.

№ п/п	Сводная информация о рассмотренных механизмах защиты данных
(0)	Не предпринимать никаких действий.
(1)	Минимальное решение позволило бы а) идентифицировать передачи, для которых закон обеспечивает адекватную защиту конфиденциальности и опубликовать соответствующий перечень; и б) ввести общие правила в договор с теми участниками экосистемы СКР, чьи передачи не были бы достаточно защищены с юридической точки зрения, предоставив службе обеспечения соблюдения обязательств единую и простую для поддержания платформу.
(2)	Можно было бы сформулировать политику защиты конфиденциальности ICANN для СКР на основе стандартной передовой практики защиты конфиденциальности, а также разработать стандартные положения договоров, которые претворяли бы эту политику в жизнь во всей экосистеме СКР. Эти стандартные положения можно было бы включить во все договора между ICANN и всеми участниками экосистемы СКР, занимающимися передачей данных, гарантируя достаточно высокий уровень защиты данных, чтобы обеспечить возможность беспрепятственной передачи данных в пределах экосистемы.
(3)	Считая ICANN многонациональной некоммерческой корпорацией, можно было бы подчинить всю находящуюся под ее контролем экосистему СКР обязательным корпоративным правилам (ОКП), которые доказали свою эффективность в обеспечении возможности передачи данных по всему миру в рамках организации. В этом случае вся экосистема становится предметом обеспечения соблюдения обязательств. ICANN могла бы рассматриваться как действующий «контролер данных», если использовать терминологию АТЭС и ЕС, определяющий политику и требования договоров.

Оценка:

Вариант (0): не предпринимать никаких действий. Учитывая рост сложности системы в мировом масштабе и важность повышения точности и подотчетности, этот вариант был признан неприемлемым.

Вариант (1): механизмы, способствующие повседневному законному сбору и передаче данных. Это вариант был бы более сложным и более динамичным по мере изменения законов в различных юрисдикциях и должен был бы учитывать сложный поток данных внутри экосистемы. Как рассматривалось ранее, отдельные владельцы регистраций могут использовать регистраторов в разных юрисдикциях, проверяющего в третьей юрисдикции и хранить данные в реестре в четвертой юрисдикции, опираясь при этом на поставщика СКР в пятой юрисдикции.

Вариант (2): стандартные положения договоров, которые были бы нацелены на гармонизацию защиты данных во всей экосистеме СКР. Выбор этого варианта потребовал бы обеспечить соблюдение применимого законодательства для указанных заинтересованных сторон, а именно владельцев регистраций, регистраторов, реестров и ICANN. Он также мог бы охватывать новых участников экосистемы СКР, рекомендованных в настоящем отчете: проверяющих, поставщика СКР, органы аккредитации пользователей СКР и т. д.

Помимо обязательного соблюдения местных законов о защите данных, этот вариант благодаря заимствованию общих элементов законодательства АТЭС и ЕС о защите данных, сделал бы многое для обеспечения соблюдения требований. В положениях договоров можно было бы определить условия согласия, права доступа, политики хранения и остальные элементы, путем включения (например) требований ЕС о законной обработке данных и соответствующие элементы обязательных корпоративных правил. Такие стандартные положения договоров не обязательно требовали бы получения разрешения/мониторинга со стороны органов защиты данных, за исключением тех юрисдикций, где подобные разрешения являются обязательными.

Вариант (3) (ОКР для экосистемы СКР): помимо обязательного соблюдения местных законов о защите данных, этот вариант позволил бы заимствовать общие элементы законодательства АТЭС и ЕС о защите данных. Как и в случае варианта (2), в положениях договоров можно было бы определить условия согласия, права доступа, политики хранения и остальные элементы, путем включения (например) требований ЕС о законной обработке данных и соответствующие элементы обязательных корпоративных правил. Такие стандартные положения договоров не обязательно требовали бы получения разрешения/мониторинга со стороны органов защиты данных, за исключением тех юрисдикций, где подобные разрешения являются обязательными. Однако ОКР потребовалось бы адаптировать к характеристикам экосистемы СКР. ОКР, пожалуй, больше применимы к юридическим лицам с традиционной структурой управления, чем к экосистеме, состоящей из слабо связанных компонентов, такой

как та, что находится под управлением ICANN, но на самом деле много-национальные корпорации обеспечивают соблюдение своих обязательных правил по защите конфиденциальности через точно такие же договора, которые использует ICANN для аккредитации своих заинтересованных сторон и контроля над ними.

В заключение, вариант «не предпринимать никаких действий» не представляется реальным, особенно в том случае, если будут приняты рекомендации ЭРГ относительно улучшения точности и подотчетности. Вариант (1) был бы достаточно сложен с юридической точки зрения и не обеспечивает равенства прав всех владельцев регистраций, в то время как вариант (3) поднимает вопросы применимости в экосистеме СКР (то есть, осуществимо ли введение обязательных корпоративных правил, будут ли они признаны, и какими были бы последствия для ICANN в плане ответственности?).

Поэтому ЭРГ рекомендует вариант (2) — разработать политику, использующую стандартные пункты договоров, которые приведены в соответствие с законами о защите данных, реализовать требования этой политики и обеспечить через различные механизмы аудита соблюдение указанных средств защиты конфиденциальности через договоры между всеми участниками экосистемы СКР, вовлеченными в обработку персональной информации.

Реализация механизмов защиты данных

Для всех перечисленных выше сценариев важен вопрос реализации СКР — особенно в плане местонахождения поставщика СКР.

Если СКР будет хранить персональные данные, то было бы удобно разместить их в такой юрисдикции, где предусмотрены осуществимые права на защиту данных, чтобы избежать вопросов, относящихся к законности передачи данных и ответственности за утечку данных. Эта проблема снимается, если СКР хранит данные в той же стране, где находится обработчик данных. Аналогичная концепция должна рассматриваться даже в том случае, если данные не хранятся в указанной стране, а передаются туда для обработки (например, проверки) и впоследствии пересылаются в какое-то другое место. ЭРГ рассмотрела три варианта реализации защиты данных:

№ п/п	Сводная информация о рассмотренных вариантах реализации защиты данных
(0)	Вариант «не предпринимать никаких действий» соответствует ситуации, когда уровень правовой защиты данных, применимый в месте нахождения СКР, не учитывается во время географического выбора. Результатом этого может стать размещение СКР в юрисдикции с низким уровнем защиты данных.
(1)	СКР могла бы обеспечить правовое обособление. В частности, элементы данных можно было бы снабдить метками, соответствующими применимому для субъекта данных (то есть владельца регистрации) законодательству, и затем обрабатывать надлежащим образом. Чтобы добиться такого правового обособления, в СКР можно было бы внедрить «обработчик правил», который при каждой конкретной передаче применял бы положения соответствующих законов о защите данных. Точнее говоря, понятие «обработчик правил» относится к функции, которую можно было бы реализовать в СКР для (а) управления хранением, сбором и обработкой информации о доменных именах с учетом юрисдикций владельца регистрации, контактного лица, регистратора, реестра и СКР (представленных следующими элементами данных: код страны владельца регистрации и контактного лица, юрисдикции регистратора и реестра), и (б) соблюдения законов о защите данных соответствующих юрисдикций, в соответствии с политикой ICANN, которая позже будет определена для СКР. Эта концепция сложна по определению, как описано выше, и трудно обеспечить ее соблюдение, если СКР находится в юрисдикции, где нет законов о защите данных, дающих возможность обратиться в суд.
(2)	Местонахождение СКР следует выбирать по критерию наиболее удобной и наименее осложненной передачи данных. Это подразумевает выбор такого места (таких мест) хранения данных СКР, где действующие национальные законы о защите данных обеспечивают максимальную степень защиты.

Оценка:

Вариант (0) «не предпринимать никаких действий» сохраняет существующее положение дел и повышает сложность многих операций передачи данных по следующим причинам:

- сохранение процесса, который делает сложным и на практике почти невозможным соблюдение законодательной базы;
- наложение административного и правового бремени на владельцев регистраций, а также на других участников экосистемы, включая отдел обеспечения соблюдения договорных обязательств ICANN; и
- почти полное отсутствие прозрачности в отношении соблюдения местных законов о защите данных и конфиденциальности, а также отсутствие масштабируемости.

Вариант (1) правовое обособление путем использования «обработчика правил» — инновационное решение, не его осуществимость с технической точки зрения необходимо проверить. Юридически, есть ряд открытых вопросов, особенно касающихся определения, правовой приемлемости и реализации такой системы.

Вариант (2) размещение данных в выбранной юрисдикции (выбранных юрисдикциях) мог бы стать элегантным и простым решением, обеспечивающим очень высокую степень защиты для всех перемещений данных. Однако сам по себе этот вариант не позволяет применять местные законы о защите данных, действующие в юрисдикции каждого субъекта.

Поскольку вариант (0) не осуществим, а варианты (1) и (2) не являются взаимоисключающими*, на данном этапе ЭРГ рекомендует рассматривать оба варианта — (1) и (2) — в качестве средств реализации высокого уровня защиты данных, который будет обеспечен благодаря политике и стандартным положениям договоров.*

После обсуждения всех вариантов, связанных с политиками, механизмами и реализацией защиты данных, ЭРГ согласовала следующие принципы:

№ п/п	Принципы защиты данных
105.	Должны быть внедрены механизмы, способствующие повседневному законному сбору данных и их передаче между участниками экосистемы СКР.
106.	Стандартные пункты договоров, приведенные в соответствие с законами о защите конфиденциальности и данных, должны быть закреплены в составе политики с обеспечением их соблюдения через договоры между всеми участниками экосистемы СКР, вовлеченными в обработку персональной информации.
107.	В качестве двух средств реализации необходимой высокой степени защиты данных необходимо рассматривать информационную систему, в которой применяются законы о защите данных (то есть «обработчик правил») и правильное размещение хранилища данных СКР. Это можно обеспечить через стандартные положения договоров, которые проистекают из грамотной политики защиты конфиденциальности для экосистемы СКР.

б. Принципы доступа правоохранительных органов к данным

В отличие от случая защиты данных, юридическую защиту субъекта данных в случае доступа правоохранительных органов нельзя «экспортировать». Что касается доступа правоохранительных органов, были рассмотрены три варианта.

№ п/п	Сводная информация о рассмотренных вариантах доступа правоохранительных органов к данным
(0)	«Не предпринимать никаких действий.» Доступ правоохранительных органов будет осуществляться по имеющимся правилам настолько, насколько национальные правоохранительные органы будут иметь доступ к данным СКР, которые находятся каждом хранилище данных на соответствующем национальном уровне. Доступ к централизованному порталу СКР будет предоставляться в соответствии с национальным законодательством страны, где размещен портал СКР.
(1)	На уровне центрального портала СКР, когда данные не являются общедоступными и когда в соответствии с применимым национальным законодательством правоохранительному органу не нужно соблюдать конкретные юридические процедуры, могут быть определены условия доступа к СКР и реализованы одним из двух способов: а) Европол и Интерпол могли бы заключить с СКР договор на создание системы, в которой они будут действующим в режиме реального времени активным посредником для всех операций доступа

№ п/п	Сводная информация о рассмотренных вариантах доступа правоохранительных органов к данным
	правоохранительных органов и будут нести ответственность за надлежащую защиту и использование данных. b) Европол и Интерпол могли бы заключить с СКР договор, согласно которому они будут выполнять функции органов аккредитации пользователей от лица сообщества правоохранительных органов, выдавая заявителям разрешения на получение учетных данных СКР, которые впоследствии отдельные правоохранительные органы будут использовать для доступа к защищенным данным СКР и нести ответственность за надлежащую защиту и использование данных.
(2)	Дополнительно, на центральном уровне, можно ввести механизмы, которые позволяли бы правоохранительному органу получать доступ к центральному порталу СКР, даже тогда, когда существуют конкретные требования установления традиционных двусторонних взаимоотношений, которые регулировались бы договорами о правовой помощи (MLAT). Разделение данных в соответствии с применимым законодательством обеспечило бы поддержку внедрения такого механизма.

Оценка:

Вариант (0) («не предпринимать никаких действий»): очевидно не принесет никакой практической пользы правоохранительным органам в плане доступа.

Вариант (2) (договора MLAT на уровне портала для доступа пользователей к СКР): не ожидается, что для доступа к какому-либо из рекомендованных защищенных элементов данных через СКР правоохранительному органу потребуется дополнительное официальное разрешение. Поэтому в дальнейшем вариант (2) можно не рассматривать.

Вариант (1) (подход на основе портала для доступа аккредитованных пользователей к СКР) облегчает задачу доступа правоохранительных органов. Хотя в основе обоих вариантов — (1a) и (1b) — находились бы уже существующие структуры, вариант (1a) (аккредитованный доступ с разделением через посредника в режиме реального времени) также был бы основан на существующих механизмах сотрудничества правоохранительных органов и позволил бы избежать повышения сложности. Однако при этом все же необходимо обеспечить возможность обнаружения и устранения потенциальных индивидуальных злоупотреблений.

Вариант (1a) дополнительно рассматривается в разделе IV(c), «Аккредитация пользователей СКР», сценарий № 3, в котором подробно рассматривается, как потенциальные органы аккредитации, такие как Интерпол, могут в качестве доверенных лиц направлять утвержденные запросы правоохранительных органов к СКР, при этом предотвращая возможные злоупотребления. Соответствующие рекомендации см. в разделе «Принципы аккредитации пользователей СКР».

Кроме того, для варианта (1) необходимо обеспечить, чтобы правовая база национального правоохранительного органа в юрисдикции (юрисдикциях), где хранятся данные СКР, не превосходила правовую базу, установленную для СКР. Поэтому географическое положение СКР является крайне важным фактором.

№ п/п	Принципы доступа правоохранительных органов
108.	СКР должна хранить данные в юрисдикции (юрисдикциях), где правоохранительные органы пользуются доверием в мировом масштабе, независимо от модели реализации.

в. Соблюдение обязательств и принципы договорных взаимоотношений

ЭРГ рекомендует следующую совокупность принципов, касающихся договорных взаимоотношений между сторонами в экосистеме СКР:

№ п/п	Принципы договорных взаимоотношений
109.	Управлять СКР должен сторонний поставщик, являющийся неправительственной организацией с мировым охватом.
110.	ICANN должна заключить соответствующие договора со сторонним поставщиком СКР, которые обеспечивали бы работоспособность, проверку и соблюдение обязательств.
111.	ICANN должна заключить соответствующие договора с проверяющими, поставщиками услуг сохранения конфиденциальности/регистрации через доверенных лиц, органами утверждения защищенных учетных данных и другими лицами, которые могут взаимодействовать с СКР (см. раздел III(c), принцип № 1).
112.	ICANN должна внести поправки в существующие соглашения (CAP, соглашения с реестрами) для включения в них положений о СКР и аннулирования устаревших требований.
113.	СКР необходимо применять ко всем реестрам рДВУ, как существующим, так и новым. Недопустимо предоставление привилегий с учетом предыдущих заслуг или особого освобождения.

г. Принципы подотчетности и аудита

ЭРГ рекомендует возложить на участников экосистемы СКР ответственность за следующие действия с регистрационными данными:

№ п/п	Принципы подотчетности и аудита
114.	Все организации в экосистеме СКР должны нести ответственность за выполнение одного или нескольких требований, изложенных в таблице 6: а) предоставление точных и надежных регистрационных данных б) использование информации только для указанной цели в) защита собранной, хранящейся или пересылаемой информации г) подтверждение или проверка подлинности информации во время ее получения д) своевременное обновление представленной ранее информации е) обеспечение соблюдение политик защиты конфиденциальности и условий использования СКР ж) обнаружение случаев неправильного обращения с регистрационной информацией з) обработка и отслеживание жалоб и) соблюдение установленных политик в отношении условий использования и условий обслуживания к) внедрение механизмов обнаружения массовой обработки данных третьей стороной и массового мошеннического создания учетных записей л) введение процедуры постоянного аудита и исправления нарушений Следующие заинтересованные стороны[25] выполняют в экосистеме СКР функции, предусматривающие ответственность: а) Пользователи СКР, стремящиеся получить данные (USD) — перечислены в разделе III б) Владельцы регистраций в) Регистраторы[26] г) Реестры[27]

[25] Эти функции и обязанности распространяются на агентов и правопреемников заинтересованных сторон (например, реселлеров)

[26] Согласно определению, которое находится по адресу http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm

[27] Согласно определению, которое находится по адресу http://newgtlds.icann.org/en/applicants/agb/agreement-approved-09jan14-en.pdf

№ п/п	Принципы подотчетности и аудита
	д) Поставщик службы каталогов регистрации е) ICANN ж) Поставщики услуг сохранения конфиденциальности или регистрации через доверенных лиц з) Орган утверждения защищенных учетных данных и) Проверяющие к) Органы аккредитации пользователей СКР л) Целевые контактные лица м) Поставщики услуг депонирования данных
115.	СКР должна создавать процедуры обработки жалоб на отсутствие данных, ненадлежащее использование данных, несанкционированный доступ к данным, нарушения политики защиты конфиденциальности и неточности в сохраненных данных; например: элементы данных контактного лица по вопросам злоупотреблений и портал для регистрации жалоб от получающих данные пользователей СКР и владельцев регистраций.
116.	СКР должна предусматривать поэтапные меры устранения неточностей в данных; например: предупреждение по электронной почте, видимые пользователю/браузеру метки записей, действия отдела обеспечения соблюдения обязательств ICANN и другие новые стимулы точности. (Требования к точности см. в разделе V «Улучшение качества данных».)
117.	СКР должна предусматривать поэтапные меры устранения несанкционированного доступа к данным; например: предупреждение по электронной почте, ограничение скорости, временное блокирование, приостановка аккредитации, лишение аккредитации и другие сдерживающие средства. (Требования к регулируемому доступу см. в разделе IV «Повышение подотчетности».)
118.	СКР должна предусматривать поэтапные меры устранения ненадлежащего использования данных; например: предупреждение по электронной почте, ограничение скорости, временное блокирование, приостановка аккредитации, лишение аккредитации и другие отрицательные стимулы. (Разрешенные цели см. в разделе III «Пользователи и цели».)
119.	СКР должна создавать механизмы аудита для обнаружения неправильного обращения с учетными данными для доступа к СКР и нарушений условий обслуживания; например: механизмы обнаружения необычной манеры поведения. (Требования к аккредитации пользователей СКР см. в разделе IV «Повышение подотчетности».)

№ п/п	Принципы подотчетности и аудита
120.	СКР должна создавать механизмы аудита для обнаружения неправильного обращения с регистрационными данными, не соответствующего заявленным целям; например: механизмы обнаружения необычной манеры поведения. (См. раздел III «Пользователи и цели».)
121.	СКР должна создавать механизмы аудита для обнаружения злоупотреблений проверяющих; например: обучение проверяющих, периодический случайный выборочный контроль данных с целью обеспечения надлежащего качества проверки. (См. раздел V «Улучшение качества данных».)
122.	СКР должна создавать механизмы аудита для обнаружения злоупотреблений органов аккредитации пользователей СКР; например: создавать механизмы обнаружения необычной манеры поведения. (Определения злоупотреблений см. в разделе IV «Повышение подотчетности».)
123.	СКР должна создавать механизмы аудита для обнаружения злоупотреблений поставщиков услуг сохранения конфиденциальности/регистрации через доверенных лиц и органов утверждения защищенных учетных данных; например: создавать механизмы обнаружения необычной манеры поведения. (Определения злоупотреблений см. в разделе VI «Улучшение защиты конфиденциальности владельцев регистраций».)
124.	Получающие данные пользователи СКР в условиях обслуживания (ToU) должны дать свое согласие на аудит доступа к данным, использование и предоставление точных сведений о своей личности и целях использования данных.
125.	СКР должна предусматривать процедуру устранения нарушений, приостановки или аннулирования соглашений с проверяющими в случае ненадлежащей проверки, хранения и защиты данных. (Требования к проверяющим см. в разделе V «Улучшение качества данных».)
126.	СКР должна предусматривать процедуру устранения нарушений, приостановки или аннулирования соглашений с органами утверждения защищенных учетных данных в случае ненадлежащего или не отвечающего требованиям утверждения. (Требования см. в разделе VII «Улучшение защиты конфиденциальности владельцев регистраций».)

№ п/п	Принципы подотчетности и аудита
127.	СКР должна предусматривать процедуру устранения нарушений, приостановки или аннулирования соглашений с органами аккредитации пользователей СКР в случае ненадлежащей аккредитации пользователей СКР, хранения и защиты их данных. (Требования к органам аккредитации пользователей СКР см. в разделе IV «Повышение подотчетности».)
128.	ICANN обязана установить политики в отношении условий обслуживания, обеспечивающие предоставление реестрами, регистраторами и проверяющими точных, обновляемых и актуальных данных в СКР. (Требования к СКР и реестрам, которые должны быть отражены в соглашениях с реестрами и САР, см. в разделе VI «Правовые и договорные факторы».)
129.	СКР должна предусматривать процедуру аудита реестров, регистраторов и проверяющих и процедуру информирования ICANN в том случае, если реестр, регистратор или проверяющий не предоставляет точных, обновляемых и актуальных данных. (Требования к СКР и реестрам, которые должны быть отражены в соглашениях с реестрами и САР, см. в разделе VI «Правовые и договорные факторы».)
130.	СКР должна предусматривать механизмы аудита для обеспечения постоянного качества и целостности данных, собранных СКР и находящихся у поставщика услуг депонирования данных. (См. раздел VIII «Хранение, депонирование и регистрация данных».)
131.	ICANN должна создать механизмы аудита для обнаружения нарушений любых условий и положений поставщиком СКР. Например: предоставление возможности несанкционированного использования данных, игнорирование жалоб на злоупотребления при использовании данных, злоупотребления в отношении учетных записей или при проверке данных. (См. раздел VI «Правовые и договорные факторы»)
132.	ICANN должна ввести процедуру устранения нарушений, приостановки или аннулирования соглашения с поставщиком СКР в случае невыполнения им своих обязательств. Например: требований к доступности, надежности, конфиденциальности, прав доступа и технических характеристик. (См. раздел VI «Правовые и договорные факторы»)
133.	ICANN должна определить ориентиры и ежегодно оценивать улучшения в плане достижения главных целей СКР: (i) улучшение качества данных, (ii) улучшение подотчетности, (iii) улучшение защиты конфиденциальности. СКР обязана демонстрировать неуклонный прогресс с одинаковыми темпами во всех трех областях, используя процедуру выявления и устранения непредвиденных проблем, способных замедлить улучшения в любой области по сравнению с другими.

В следующей таблице в развитие принципа № 114 приведена сводная информация о субъектах экосистемы СКР, видах подотчетности и требованиях к аудиту, которые должны применяться по отношению к ним.

Применимые требования	Пользователь СКР, желающий получить данные	Владелец регистрации	Регистратор	Реестр	Поставщик СКР	ICANN	Поставщик услуг сохранения конфиденциальности	Ответственный за утверждение защищенных учетных данных	Проверяющий	Ответственный за аккредитацию пользователей СКР	Целевое контактное лицо	Поставщик услуг депонирования данных
Предоставление точных и надежных данных		✔	✔	✔	✔		✔	✔	✔		✔	✔
Целевое использование	✔		✔	✔	✔	✔	✔	✔	✔			✔
Защищенная информация			✔	✔	✔	✔	✔	✔	✔			✔
Подтверждение/ аутентификация					✔				✔	✔		
Своевременное обновление		✔	✔	✔			✔	✔	✔		✔	
Обеспечение соблюдения политики конфиденциальности			✔	✔	✔	✔	✔	✔	✔			✔
Обнаружение злоупотреблений					✔	✔				✔		
Процедура рассмотрения жалоб			✔	✔	✔	✔	✔	✔	✔	✔		
Недопущение сбора данных третьими лицами				✔	✔				✔			
Аудит и исправление нарушений					✔	✔				✔		

Таблица 6. Требования к соблюдению обязательств субъектами экосистемы СКР

VII. Улучшение защиты конфиденциальности владельцев регистраций

Центральным в круге обязанностей ЭРГ является вопрос о том, как разработать систему, повышающую точность собранных данных и одновременно предлагающую средства защиты владельцам регистраций, которые стремятся защитить и сохранить свою конфиденциальность. ЭРГ признает, что личная информация защищена законами о защите данных и даже в отсутствие соответствующего законодательства у частных лиц есть законные причины стремиться к повышению защиты своей личной информации. Кроме того, некоторые компании и организации могут стремиться к защите своей информации для законных целей, например, на этапе подготовки к началу производства новой линейки продуктов или, в случае малого бизнеса, когда контактная информация содержит личные данные.

Соответственно, ЭРГ рекомендует следующие основные принципы:

№ п/п	Принципы защиты конфиденциальности
134.	Помимо конфиденциальности, обеспечиваемой в соответствии с законами о защите данных, в экосистеме СКР также должны учитываться потребности в конфиденциальности путем включения в ее состав: • аккредитованных услуг сохранения конфиденциальности и регистрации через доверенных лиц для общей защиты личных данных и соблюдения местных законов о неприкосновенности частной жизни; и • аккредитованных услуг защиты учетных данных для использования лицами, которые подвергаются опасности, а также в условиях лишения права на свободу слова или преследования мнений.
135.	Необходимы аккредитация поставщиков услуг сохранения конфиденциальности/регистрации через доверенных лиц и правила, касающиеся предоставления и использования аккредитованных услуг сохранения конфиденциальности/регистрации через доверенных лиц.
136.	За рамками регистрации доменных имен через аккредитованных поставщиков услуг сохранения конфиденциальности/регистрации через доверенных лиц все владельцы регистраций должны взять на себя ответственность за регистрируемые ими доменные имена.
137.	ICANN должна изучить возможность выработки единой гармонизированной политики соблюдения конфиденциальности, обеспечивающей всестороннее регулирование деятельности СКР, как рассматривается ниже.

Помимо законов о защите данных, другие национальные законы о неприкосновенности частной жизни и конституции защищают права миллионов пользователей Интернета свободно высказываться в Интернете и выражать свои мнения в отсутствие простой и мгновенной возможности отследить их имена и адреса. К этим законам о неприкосновенности частной жизни относится Декларация прав человека ООН (статья 19),[28] которая защищает права на свободу самовыражения и свободу слова, а также сохраняет возможность и даже обязанность групп, организаций, физических лиц и компаний (таких как СМИ и периодические издания) анализировать и подвергать критике методы руководства, осуществления лидерства и управления страной, культурой или обществом.

Законы о неприкосновенности частной жизни, защищающие свободу самовыражения, часто признают необходимость реализации этих прав на основе принципов невозможности установления связи между наименованиями и адресами организаций или групп и их высказываниями, которые могут содержать критику в адрес правительства, общества, сообщества или ближайшего окружения. Они могут поощрять создание рынка идей и ставить потребности открытых обществ в общении выше полномочий преследования выразителей мнений или возможности предвзятого отношения к высказыванию просто по причине личной неприязни к его автору.

Законы о неприкосновенности частной жизни и конституционные права также могут защищать свободу союзов, вероисповедания, этнической принадлежности, морали и сообществ. В совокупности, они могут устранять необходимость того, чтобы физические лица или организации называли свои имена или даже адреса при выражении непопулярных мнений или мнений меньшинства — чтобы не было возможности мгновенно их обнаружить и опорочить или нанести еще больший вред. В это десятилетие, когда наблюдаются политические волнения широких масс и неприятие любых противоположных мнений, законы о неприкосновенности частной жизни защищают мнения меньшинства и сохраняют мощную возможность авторов публикаций в Интернете настаивать на изменениях и реформах.

Упоминая в настоящем отчете о конфиденциальности и защите персональной информации, мы хотим признать обе эти отдельные группы прав, защиту которых часто обеспечивает разное законодательство и очень по-разному в различных странах мира.

a. Принципы использования аккредитованных услуг сохранения конфиденциальности и регистрации через доверенных лиц

В настоящее время предлагаются услуги, позволяющие скрыть личность и/или адреса субъектов, использующих доменные имена. Они возникли по причине открытого характера WHOIS. Хотя существует множество вариантов, в Соглашении об аккредитации регистраторов 2013 года определены две таких услуги:

- «Услуга сохранения конфиденциальности» — это услуга, посредством которой зарегистрированное доменное имя регистрируется на пользователя-бенефициара как на владельца зарегистрированного имени, для которого поставщиком услуг сохранения конфиденциальности и регистрации через доверенных лиц предоставляется другая надежная контактная информация для отображения контактной информации владельца зарегистрированного имени в службе регистрационных данных (WHOIS) или в других подобных службах.
- «Услуга регистрации через доверенных лиц» — это услуга, посредством которой владелец зарегистрированного имени предоставляет клиенту поставщика услуг сохранения конфиденциальности и регистрации через доверенных лиц право пользоваться зарегистрированным доменным именем, а в службе регистрационных данных (WHOIS) или в других подобных службах вместо контактной информации клиента поставщика услуг сохранения конфиденциальности и регистрации через доверенных лиц отображается контактная информация владельца зарегистрированного имени.

В этих определениях «Поставщик услуг сохранения конфиденциальности и регистрации через доверенных лиц» или «Поставщик услуг» — это поставщик указанных видов услуг, в том числе Регистратор и аффилированные с ним лица, в зависимости от ситуации. «Клиент поставщика услуг сохранения конфиденциальности и регистрации через доверенных лиц» означает (независимо от терминологии, используемой поставщиком услуг сохранения конфиденциальности и регистрации через доверенных лиц) владельца лицензии, клиента, пользователя-бенефициара, бенефициара или другое лицо, пользующееся услугами сохранения конфиденциальности и регистрации через доверенных лиц.

Сегодняшние услуги сохранения конфиденциальности и регистрации через доверенных лиц не стандартизированы; у поставщиков нет договорных

взаимоотношений с ICANN, хотя в CAP 2013 вводится концепция аккредитации корпорацией ICANN и основные обязательства, которые отражены во Временной спецификации. Однако некоторые поставщики также являются регистраторами. Все регистраторы подчиняются положениям CAP, где относительно доменных имен, зарегистрированных через доверенных лиц, сказано следующее:[29]

> 3.7.7.3 Любой владелец зарегистрированного имени, намеревающийся предоставить лицензию на использование доменного имени третьей стороне, все равно является владельцем зарегистрированного имени и отвечает за предоставление своей полной контактной информации и за предоставление и обновление точной информации о контактном лице по техническим и административным вопросам, достаточной для обеспечения своевременного разрешения *любых проблем, возникающих*[30] в связи с зарегистрированным именем. Владелец зарегистрированного имени, лицензирующий использование зарегистрированного имени согласно данному положению, принимает на себя ответственность за ущерб, нанесенный неправомерным использованием зарегистрированного имени, если он в течение семи (7) дней не раскроет текущую контактную информацию, предоставленную лицензиатом, и личность лицензиата стороне, предоставившей владельцу зарегистрированного имени разумные доказательства вреда.

Данные WHOIS для доменного имени, зарегистрированного сегодня через доверенное лицо, может выглядеть следующим образом:

```
Domain Name: EXAMPLE-DOMAIN.COM
    Created on: 31-Oct-11
    Expires on: 31-Oct-13
    Last Updated on: 19-Sep-12

 Registrant:
 Domains By Proxy, LLC                        ← Registrant Name = Proxy
 DomainsByProxy.com                           ← Registrant Org = Proxy
 14747 N Northsight Blvd Suite 111, PMB 309   ← Registrant Address = Proxy's
 Scottsdale, Arizona 85260
 United States

 Admin Contact: [same for Tech Contact]
    Private, Registration
    example-domain.com @domainsbyproxy.com          ← Email = domain@proxy
    Domains By Proxy, LLC                           ← Name = Proxy
    DomainsByProxy.com                              ← Org = Proxy
    14747 N Northsight Blvd Suite 111, PMB 309      ← Address = Proxy's
```

[29] 27 июня 2013 года Правлением ICANN было утверждено новое CAP 2013; раздел 3.7.7.3 (который здесь цитируется) остался в целом без изменений по сравнению с положением CAP 2009, за исключением добавления 7-дневного срока.

[30] Примечание: ЭРГ предлагает ICANN рассмотреть, не является ли определение «любых проблем» слишком широким.

```
Scottsdale, Arizona 85260
United States
(480) 624-2599      Fax -- (480) 624-2598      ← Tel/Fax = Proxy's
```

Данные WHOIS для доменного имени, зарегистрированного сегодня через то, что в настоящее время называется услугой сохранения конфиденциальности, выглядит аналогичным образом, за исключением того, что в качестве имени владельца регистрации (и часто в качестве имен контактов по административным/ техническим вопросам) прямо указывается имя клиента службы сохранения конфиденциальности, а не поставщика услуг регистрации через доверенных лиц.

В настоящее время нет стандартных процедур, которые использовались бы всеми существующими сегодня поставщиками услуг сохранения конфиденциальности и регистрации через доверенных лиц. Однако есть несколько общих потребностей, которые часто удовлетворяются в определенной степени:

- Переадресация сообщений клиенту сегодняшнего поставщика услуг сохранения конфиденциальности или регистрации через доверенных лиц — часто представляет собой автоматическую пересылку сообщений электронной почты, отправленной в адрес контактных лиц по административным/техническим вопросам. Переадресация выполняется многими, но не всеми поставщиками.
- Раскрытие личности владельца лицензии и контактных данных для прямой связи с клиентом поставщика услуг регистрации через доверенных лиц в ответ на жалобу, относящуюся к этому доменному имени. Процедуры, документация, быстрота реагирования и принимаемые меры различны и часто зависят от отношений между инициаторами запросов и поставщиками.
- Раскрытие личности владельца лицензии, открытое опубликование имени и контактных данных клиента поставщика услуг регистрации через доверенных лиц в WHOIS.
- Когда инициаторам запросов не удается связаться с клиентом поставщика услуг регистрации через доверенных лиц или добиться разрешения вопроса через этого поставщика, они часто обращаются к регистратору (который может быть или не быть аффилированным лицом поставщика услуг регистрации через доверенных лиц).

Недостатки сегодняшних услуг сохранения конфиденциальности и регистрации через доверенных лиц хорошо отражены в документах.[31] Для удовлетворения потребностей как владельцев регистрации доменных имен, так и заинтересованных сторон в более единообразных и надежных услугах сохранения конфиденциальности и регистрации через доверенных лиц, улучшающих подотчетность, ЭРГ рекомендует следующие принципы:

№ п/п	Принципы использования аккредитованных услуг сохранения конфиденциальности/регистрации через доверенных лиц
	Общие
138.	ICANN должна осуществлять аккредитацию поставщиков услуг сохранения конфиденциальности и регистрации через доверенных лиц[32].
139.	Как минимум, программа аккредитации должна сохранить обязательства поставщиков услуг сохранения конфиденциальности/регистрации через доверенных лиц, перечисленные в Спецификации САР 2013.
	Принципы для аккредитованных услуг сохранения конфиденциальности
140.	Юридические и физические лица имеют право регистрировать доменные имена с использованием аккредитованных поставщиков услуг сохранения конфиденциальности, которые раскрывают контактные данные владельца регистрации только в определенных ситуациях (например, при нарушении условий обслуживания, получении судебной повестки).
141.	ICANN должна потребовать включения конкретных положений в условия обслуживания. Условия обслуживания должны содержать требование к поставщику услуг прилагать усилия по доставке уведомлений в случае ускоренной приостановки функционирования доменных имен.
142.	Аккредитованные поставщики услуг сохранения конфиденциальности обязаны сообщать регистратору (используя ЦКЛ, созданное через проверяющего) точные и надежные контактные данные для всех целевых контактных лиц, позволяющие связаться с поставщиком услуг сохранения конфиденциальности и субъектами, уполномоченными решать технические, административные и прочие вопросы от имени владельца регистрации.

[31] Список исследований и отчетов, описывающих недостатки WHOIS и услуг сохранения конфиденциальности/регистрации через доверенных лиц, см. в **Приложении В**.

[32] ОПРИ сформировала рабочую группу для разработки политик аккредитации поставщиков услуг сохранения конфиденциальности/регистрации через доверенных лиц. ЭРГ рекомендует использовать в СКР все основные принципы, сформулированные этой рабочей группой (РГ PPSAI), изменив их необходимым образом для отражения способов доступа и элементов данных СКР — что прежде всего касается опубликования данных целевых контактных лиц поставщиков КД.

№ п/п	Принципы использования аккредитованных услуг сохранения конфиденциальности/регистрации через доверенных лиц
143.	Аккредитованных поставщиков услуг сохранения конфиденциальности необходимо обязать пересылать владельцу регистрации, поступившие в его адрес сообщения электронной почты.
	Принципы для аккредитованных услуг регистрации через доверенных лиц
144.	Юридические и физические лица имеют право регистрировать доменные имена с использованием аккредитованных поставщиков услуг регистрации через доверенных лиц, которые регистрируют доменные имена по поручению своего клиента.
145.	Аккредитованные поставщики услуг регистрации через доверенных лиц обязаны сообщать регистратору (используя ЦКЛ, созданное через проверяющего) свое собственное наименование как владельца регистрации и свои контактные данные, в том числе уникальный адрес для пересылки электронной почты при необходимости связаться с организацией, уполномоченной на регистрацию доменного имени по поручению клиента службы регистрации через доверенных лиц.
146.	Являясь владельцами зарегистрированных доменных имен, аккредитованные поставщики услуг регистрации через доверенных лиц обязаны взять на себя все обычные обязанности владельцев зарегистрированных доменных имен, в том числе обязанность предоставлять точную и надежную необходимую информацию о целевых контактных лицах и остальные регистрационные данные.
147.	Аккредитованные поставщики услуг регистрации через доверенных лиц обязаны сообщать регистратору (используя ЦКЛ, созданное через проверяющего) точные и надежные контактные данные для всех целевых контактных лиц, позволяющие связаться с поставщиком услуг регистрации через доверенных лиц и субъектами, уполномоченными решать технические, административные и прочие вопросы от имени клиента этого поставщика услуг.
148.	Аккредитованных поставщиков услуг регистрации через доверенных лиц необходимо обязать пересылать поступившие в адрес владельца регистрации сообщения электронной почты, как дополнительно описано в Приложении Н.
149.	Аккредитованных поставщиков услуг регистрации через доверенных лиц необходимо обязать своевременно реагировать на требования о раскрытии сведений, как описано в процедурах решения проблем в Приложении Н.

б. Принципы использования защищенных учетных данных

Было признано, что некоторые физические лица и группы, желающие сохранить свою анонимность в Интернете, или по крайней мере избежать доступа к своему адресу и персональным данным тех лиц, которые могут представлять для них угрозу, имеют законную потребность в усиленной защите конфиденциальности. Эти стороны могут реализовать свои права в рамках законодательства о защите конфиденциальности, где оно существует, или воспользоваться услугами регистрации через доверенных лиц. Но, к сожалению, эти механизмы могут оказаться недостаточно надежными для защиты лиц, которые действительно находятся под угрозой. Если контактные данные владельца регистрации отсутствуют в Интернете, преследователи этих физических лиц или групп изберут своей целью проверяющих, регистраторов или реестры, требуя предоставить информацию и часто используя для этого психологические атаки, для отражения которых у этих сторон недостаточно средств.

Цель предоставления таких защищенных учетных данных состоит в том, чтобы обеспечить возможность анонимной регистрации для физических лиц или групп, находящихся под угрозой. К этим лицам могут относиться те, кто желает реализовать свое право на свободу слова (которая по праву считается подлежащей защите) или те, кто находится в ситуации, когда идентификация выражающего свое мнение человека может угрожать его жизни или жизни членов его семьи.

Ниже приводится пять различных примеров:

1. **Религиозные меньшинства**

   Во многих юрисдикциях есть религиозные меньшинства, которым угрожают группы более широкого населения или другие конфессии в рамках их собственной веры. Они могут выразить желание создать свой веб-сайт для предоставления информации своим членам, сохраняя при этом секретность в отношении места и способа ведения своей деятельности. Например, римская синагога не раскрывает своего адреса из-за часто возникающей угрозы террористических взрывов, но публикует время проведения служб для тех, кто знает о ее местонахождении.

2. **Бытовое насилие**

   Во многих юрисдикциях предоставляется возможность в том или ином виде изменить свою личность тем, кто подвергся бытовому насилию или сумел скрыться от субъекта преступного нападения. Кроме того, это распространяется на лиц, покинувших определенные религиозные сообщества и культы,

а также на участников программы защиты свидетелей. Защитникам женщин, подвергающихся домашнему насилию, может потребоваться реклама своих услуг в Интернете и предоставление реальным жертвам безопасных мест контакта и указаний о том, как добраться до укрытия и т. п. У физических лиц и семей, изменивших свою личность, может возникнуть законное желание создавать веб-сайты, не раскрывая свои адреса и личность. Следует отметить, что в органах государственной власти работает много людей, действующих под другим именем по разным причинам, обычно связанным с национальной безопасностью и поддержанием правопорядка, и этим людям тоже нужна расширенная защита как в своей профессиональной деятельности, так и в личной жизни.

3. Политическая свобода слова

В нескольких странах мира оппозиционные партии или проигравшие кандидаты могут столкнуться с необходимостью спасаться бегством после выборов. Они также могут захотеть создать свой веб-сайт, где будут сообщать подробности о событиях в своей стране или гонениях, которым они подвергаются. Облеченное властью правительство может преследовать этот веб-сайт, выдвигая обвинения в государственной измене или других преступлениях, после опубликования на веб-сайте документации с описанием злоупотреблений действующей власти. Это очень щекотливые ситуации, поскольку права на свободу слова сильно отличаются в разных государствах и редко выдерживают обвинения в государственной измене. Право на регистрацию домена — это все, о чем следует беспокоиться ICANN и ее аккредитованным регистраторам.

4. Этнические или другие социальные группы

Этнические группы часто подвергаются оскорблениям и дискриминации, и у них может возникнуть желание создать веб-сайты для опубликования информации, которая крайне необходима их членам. Например, у них может возникнуть желание создать веб-сайт, где члены этих групп могли бы размещать сообщения об оскорблениях, не опасаясь, что их личность будет установлена и они подвергнутся репрессиям. Другие группы, например геи, лесбиянки, транссексуалы или трансвеститы могут захотеть создать вполне обычный информационный веб-сайт для своего сообщества, но при этом будут бояться идентификации членов этих групп из-за ограничительных законов своей страны или расправы со стороны непримиримых борцов и враждебных групп. Есть случаи расправы даже с операторами веб-сайтов,

предоставляющих информацию о здоровье и питании для женщин, сведения о репродуктивных правах и т. п.

5. Журналисты, работающие на вражеской территории

У журналистов, которые публикуют репортажи, находясь на вражеской территории, может возникнуть необходимость или желание создать веб-сайт, сохранив при этом свою безопасность и конфиденциальность имени и адреса, в том числе своих коллег, переводчиков и т. д.

Изучение технологий защиты учетных данных

На рынке предлагается множество технологий защиты учетных данных, например U-Prove компании Microsoft (http://research.microsoft.com/en-us/projects/u-prove/) и Identity Mixer компании IBM (http://researcher.watson.ibm.com/researcher/-view_project.php?id=664). Эти подходы позволяют получателю доказать наличие у него различных признаков — например, что он или она были признаны и аутентифицированы заслуживающим доверия органом, что они оплатили определенное право на получение услуги — не сообщая никаких сведений о себе и не предоставляя никакой возможности отследить операции, благодаря которым они получили эти признаки. У предоставляющих эти услуги сторон есть надежное криптографическое доказательство того, что субъект, которому выдаются защищенные учетные данные, получил разрешение надежного органа, и нет необходимости знать, кто этот субъекты и как он получил это разрешение.

Такая технология могла бы использоваться для внедрения процедуры, посредством которой подвергающиеся риску субъекты, которые описаны выше, могли бы получать доменные имена, зарегистрированные с помощью защищенных учетных данных. При этом ни у регистратора, ни у проверяющего не было бы сведений о том, что за субъекты подвергаются риску, кроме контактных данных, необходимых для решения вопросов в системе DNS. Поэтому они могли бы с полным основанием не отвечать на запросы личных данных или информации об адресе. Безусловно, есть поводы для беспокойства в плане соблюдения технических требований, устранения злоупотреблений и указанных рисков (которые рассматриваются ниже). Ключевым моментом здесь является то, что для доменных имен, которые зарегистрированы с использованием защищенных учетных данных, регистраторы и реестры больше не несут риск ответственности за идентификацию личности уязвимых людей перед нападающей стороной.

Функциональные проблемы

Чтобы выявить проблемы и риски, связанные с такой услугой, ЭРГ изучила следующие возможные ситуации:

1. Инициатор запроса информации желает определить настоящее имя или адрес физического лица, как описано в пунктах 2, 3 и 4 выше, для тех целей, которые он представляет как законные (обвинения в нарушении прав на товарные знаки, желание купить или продать доменное имя, стремление изучить безопасность продукта и т. п.). Следует обратить внимание, что в ситуации борьбы на не жизнь, а на смерть, регистратор находится в трудном положении, когда пытается определить, не обманывает ли его инициатор запроса, и невозможно ожидать от персонала понимания того, с какой неизвестной угрозой могут столкнуться люди, особенно в случае изменения личности.

2. Инициатор запроса обращается к регистратору (или назначенному проверяющему ЦКЛ) с обвинениями в преступной или клеветнической деятельности, и требует уничтожить веб-сайт, использующий это доменное имя. В таких ситуациях будут соблюдаться условия обслуживания, предложенные регистратором или поставщиком услуг регистрации через доверенных лиц, что может привести к отправке запроса на раскрытие сведений о личности и адресе владельца лицензии на доменное имя. Однако для доменных имен, зарегистрированных с использованием защищенных учетных данных, успешно выполненный запрос на раскрытие сведений позволит получить доступ только к доверенному органу, который утвердил защищенные учетные данные. На данном этапе доверенный орган будет нести ответственность за расследование потенциального злоупотребления в DNS. В некоторых случаях, таких как преступная деятельность, возможно, будет разрешено ускоренное удаление этих веб-сайтов.

3. В тех случаях, когда государственные органы выдвигают обвинения в том, что политическая свобода слова поднялась до уровня государственной измены или других преступлений, регистраторы, возможно, тоже будут вынуждены в ускоренном порядке удалять веб-сайты, использующие доменные имена, которые зарегистрированы с помощью защищенных учетных данных, в зависимости от соответствующего законодательства или юрисдикции.

Даже с учетом этих ограничений, защищенные учетные данные обеспечили бы гораздо большую безопасность подвергающихся риску субъектов, чем сейчас, и

если новая СКР будет требовать большей точности данных и ответственности, то такая услуга, как эта, будет необходима. Чтобы выполнить это, необходимо разработать следующие ключевые функциональные элементы:

1. Процедура для определения критериев признания права субъекта, подвергающегося риску, на получение защищенных учетных данных, начиная с перечисленных выше примеров пользователей, а также всех остальных, которых сообщество ICANN признает правомочными через разработку политики.
2. Формы заявок, необходимые формальные подтверждения и финансовые системы, в центре которых находится обеспечение защиты личности субъектов, подвергающихся риску (и в некоторых случаях лиц, удостоверивших это). В любой анонимной системе это является одним из основных слабых мест.
3. Независимая ревизионная комиссия для оценки и утверждения заявок на защищенные учетные данные и аттестации доверенных лиц, например государственных органов, разрешивших смену имени, организаций ООН, принимающих участие в защите беженцев, международных союзов журналистов и т. д.
4. Доверенные стороны (например те, которые перечислены в пункте № 3 выше), которые хотят быть посредниками при передаче этой независимой ревизионной комиссии заявок на защищенные учетные данные и при получении зарегистрированных в итоге доменных имен. Эти доверенные лица — далее именуемые получателями защищенных учетных данных — должны засвидетельствовать необходимость получения подвергающимся риску субъектом защищенных учетных данных и взять на себя ответственность за любое потенциальное злоупотребление в DNS, связанное с использованием доменных имен, которые были зарегистрированы с использованием этих защищенных учетных данных.
5. Аккредитованные поставщики услуг регистрации через доверенных лиц, готовые принимать защищенные учетные данные при регистрации доменных имен, лицензия на которые получена у органа утверждения защищенных учетных данных, наряду с финансовыми системами оплаты регистрации.
6. Политики, связанные с процедурами ускоренного удаления доменных имен и другими способами устранения злоупотреблений в

DNS. Сюда можно отнести расширенный контроль безопасности доменных имен, зарегистрированных с использованием защищенных учетных данных, для противодействия возможному ненадлежащему использованию DNS и злоупотреблениям, а также для содействия защите доменных имен от нападений. Стороны, заявляющие о злоупотреблениях в DNS, излагали бы свои доводы комиссии, которая утвердила заявку подвергающегося риску субъекта, и орган утверждения защищенных учетных данных оценивал бы обвинения в злоупотреблениях.

На следующем рисунке проиллюстрированы возможные взаимоотношения между этими сторонами, их обязанности и поток коммуникации между ними.

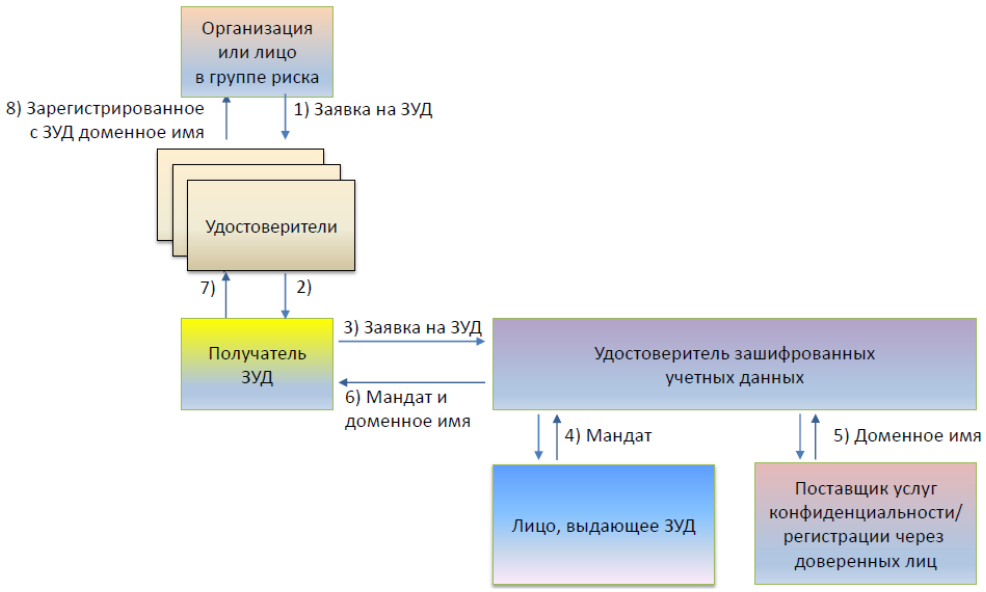


Рис. 8. Модель защищенных учетных данных

Остаточные риски

Защищенные учетные данные не получили широкого распространения, потому что, наряду с другими причинами, их сложно реализовать, особенно в том, что касается регистрации и аннулирования. Выдвигались аргументы в пользу того, что все стороны должны иметь право на такую регистрацию, однако с учетом объема работ, минимально необходимых для внедрения такой службы и обеспечения того, чтобы она не использовалась для мошеннических или преступных целей, ЭРГ считает этот подход неосуществимым. ЭРГ рекомендует проработать вариант ограниченного применения защищенных учетных данных после доказательства того, что желающие воспользоваться данной услугой лица действительно имеют законную потребность в анонимности.

Она также признает, что после регистрации такого доменного имени и ввода в эксплуатацию веб-сайта, различные виды интернет-трафика, содержащего мета-данные и информационное наполнение сайта, могут привести к идентификации пользователя доменного имени. Это не имеет отношения к деятельности ICANN, посвященной исключительно вопросам регистрации доменов и сопровождения данных, которые собираются, используются и раскрываются для достижения определенных целей, входящих в круг обязанностей ICANN. Информация, созданная во время фактического использования доменного имени, должна входить в сферу ответственности организаций, подающих заявки и использующих доменные имена, зарегистрированные с помощью защищенных учетных данных, и, возможно, важно предоставлять им информацию, подчеркивающую наличие такого риска. Сфера ответственности ICANN ограничена рамками самой системы доменных имен.

№ п/п	Принципы защиты учетных данных
150.	Частные лица и группы, которые могут продемонстрировать, что окажутся под угрозой в случае их идентификации должны иметь возможность анонимно подавать заявки и получать зарегистрированные доменные имена с использованием защищенных учетных данных при содействии органов аттестации и доверенных третьих лиц, создающих защитный экран между находящимися под угрозой субъектами и регистраторами/проверяющими.
151.	ICANN должна способствовать созданию независимой заслуживающей доверия ревизионной комиссии, которая будет осуществлять проверку заявлений организаций или частных лиц о том, что они подвергаются

№ п/п	Принципы защиты учетных данных
	риску, для утверждения (и в необходимых случаях аннулирования) учетных данных. Такая организация — называемая в дальнейшем органом утверждения защищенных учетных данных (SCA) — обязана развивать предоставление других услуг, например услуг обучения пользователей по вопросам рисков и практики безопасной работы в Интернете.
152.	ICANN должна способствовать созданию или лицензированию органа выдачи защищенных учетных данных, признающего положительные решения SCA и генерирующего соответствующие защищенные учетные данные.
153.	Орган утверждения защищенных учетных данных обязан использовать выданные защищенные учетные данные для получения обычным способом лицензий на использование доменных имен у аккредитованных поставщиков услуг регистрации через доверенных лиц. Сведения о поставщике услуг регистрации через доверенных лиц будут отражены в СКР. СКР не будет располагать информацией о подвергающемся риску субъекте, который использует защищенные учетные данные, и при этом должна использоваться какая-то система анонимных платежей или оплаты по доверенности.
154.	Для доменных имен, зарегистрированных с помощью защищенных учетных данных, должны соблюдаться стандартные процедуры поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц, используемые для раскрытия сведений и прекращения обслуживания. Неполучение своевременного ответа от клиента, пользующегося услугой сохранения конфиденциальности/регистрации через доверенных лиц (то есть от органа утверждения защищенных учетных данных), или доказательство злоупотребления в DNS может стать причиной ускоренного удаления доменных имен, зарегистрированных с использованием защищенных учетных данных.
155.	Признавая, что зарегистрированные с помощью защищенных учетных данных доменные имена сами подвержены риску кибератак, или то, что расследование нарушений будет сопряжено с трудностями, следует рассмотреть возможность усиленного мониторинга безопасности этих доменных имен для снижения риска.
156.	Следует сформировать политики и процедуры утверждения и аннулирования заявок на защищенные учетные данные. • Процедура утверждения должна предусматривать нулевое или

№ п/п	Принципы защиты учетных данных
	большее количество удостоверяющих лиц, необходимое для достаточной защиты личности и местонахождения подвергающегося риску субъекта, от доверенного получателя защищенных учетных данных, который подает заявку в SCA. Количество и личность удостоверяющих лиц прозрачны для СКР; единственной стороной, которая напрямую взаимодействует с SCA, является получатель защищенных учетных данных. • Процедура аннулирования должна предусматривать аналогичную защиту личности и местонахождения подвергающегося риску субъекта, обеспечивая при этом соблюдение условий обслуживания при предоставлении защищенных учетных данных. SCA должен нести ответственность за расследование обвинений в злоупотреблениях, совершенных в DNS с использованием защищенных учетных данных, и обеспечивать соблюдение условий обслуживания. Если совершенное в DNS злоупотребление достаточно серьезное и требует аннулирования учетных данных, SCA обязан привлечь получателя защищенных учетных данных к ответственности.

в. Сводная информация о ключевых преимуществах в плане конфиденциальности

При повышении точности и ответственности еще большую важность обретет защита отдельных граждан, особенно уязвимых. Внедрение принципов и механизмов защиты данных, использования аккредитованных поставщиков услуг сохранения конфиденциальности/регистрации через доверенных лиц и защищенных учетных данных в качестве неотъемлемой части СКР следующего поколения улучшит защиту конфиденциальности владельцев регистраций и контактных лиц.

Рекомендованные ЭРГ принципы защиты данных позволили бы:

- повысить единообразие защиты персональных данных за счет применения единой гармонизированной политики СКР, согласованно реализуемой во всей экосистеме СКР и использующей «обработчик правил» для применения местного законодательства;
- требовать обеспечения открытого и анонимного доступа к меньшему количеству регистрационных и контактных данных;

- лучше защитить данные о владельце регистрации и контактных лицах от неправомерного использования.

Рекомендованные ЭРГ принципы для аккредитованных поставщиков услуг сохранения конфиденциальности/регистрации через доверенных лиц позволили бы:

- внести большую ясность для владельцев регистраций, желающих воспользоваться услугами сохранения конфиденциальности/регистрации через доверенных лиц, благодаря созданию системы аккредитации поставщиков, предлагающих такие услуги;
- требовать идентификации доменного имени, как зарегистрированного с использованием аккредитованного поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц;
- четко указывать в составе регистрационных данных способы связи с поставщиком услуг сохранения конфиденциальности/регистрации через доверенных лиц;
- предотвращать использование контактных данных аккредитованного поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц третьими сторонами без разрешения.
- требовать от аккредитованного поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц пересылать электронную почту соответствующему владельцу регистрации и реагировать на запросы;
- обеспечить более согласованные и предсказуемые перспективы взаимодействия с правоохранительными органами и другими сторонними лицами, направляющими сообщения о злоупотреблениях и требования раскрыть информацию.

Рекомендованные ЭРГ принципы использования защищенных учетных данных позволили бы:

- впервые создать процедуры, позволяющие уязвимым и ущемленным в правах группам воспользоваться множеством преимуществ, которые дает владение собственными доменными именами в Интернете;
- защитить тех, кому более всего необходимо использовать Интернет для реализации права на свободу слова и общения участников группы друг с другом, предусмотрев при этом средства устранения возможных злоупотреблений;

- снять с проверяющих и регистраторов потенциальную ответственность, которую они несут сегодня за раскрытие конфиденциальных сведений личного характера в результате психологических атак;
- повысить безопасность благодаря регистрации доменных имен с использованием защищенных учетных данных;
- требовать ускоренного удаления зарегистрированных с использованием защищенных учетных данных веб-сайтов, которые используют DNS ненадлежащим образом.

VIII. Возможные модели СКР

a. Принципы разработки моделей

В настоящем отчете представлены сведения о нескольких альтернативных моделях, изученных ЭРГ, а также анализ того, каким образом эти модели могли бы обеспечить соблюдение рекомендованных ЭРГ принципов. Для оценки всех моделей использовалась совокупность разносторонних критериев, которые описаны в Приложении F.

При проведении анализа ЭРГ применяла следующие принципы разработки:

№ п/п	Принципы разработки моделей
157.	**Сбор:** Сегодня регистраторы или аффилированные с регистраторами лица собирают и хранят регистрационные данные, полученные от своих клиентов (владельцев регистраций). Этот процесс по своей природе является распределенным. Помимо продолжения накопления регистраторами или аффилированными лицами регистрационных данных, предоставленных владельцами регистраций, ЭРГ предлагает осуществлять сбор контактных данных силами проверяющих.
158.	**Хранение:** Существует множество возможных моделей хранения регистрационных данных всей совокупности рДВУ. ЭРГ выявила несколько возможных моделей, заострила внимание на двух, оказавшихся наиболее многообещающими, и выбрала одну рекомендуемую модель, применив критерии оценки, которые отражены в Приложении F.

№ п/п	Принципы разработки моделей
159.	**Доступ:** В интересах защиты конфиденциальности субъектов данных, централизованный интерфейс должен позволять надлежащим инициаторам запросов получать доступ к регистрационным данным всей совокупности рДВУ, включая нерегулируемый доступ к открытым данным и доступ аккредитованных пользователей к закрытым данным на основе проверки подлинности.
160.	**Протокол:** СКР должна использовать RDAP[33] или EPP (в зависимости от интерфейса в каждом случае) в качестве основного протокола доступа к каталогу для получения регистрационных данных из мест хранения, где бы они ни находились.

б. Рассмотренные модели

Чтобы протестировать альтернативные модели системы, рассмотренные ЭРГ в ее первоначальном отчете, и дополнительные модели, предложенные сообществом ICANN, ЭРГ сначала определила, какие модели следует подвергнуть глубокому анализу. Каждая из моделей отличается от других по многим параметрам, в том числе по способу копирования или запроса регистрационных данных в СКР. Эти различия обобщены в приведенной ниже таблице[34] и дополнительно разъясняются в Приложении F.

ВОЗМОЖНЫЕ МОДЕЛИ	Сбор	Хранение	Копирование	Доступ
Существующая WHOIS	RR	RR/Ry	н/п	RR/Ry
Интегрированная	RR и V	RR/Ry и V	н/п	СКР
Синхронизированная*	RR и V	RR/Ry и V	СКР	СКР
Региональная	RR и V	RR/Ry и V	Региональное	СКР
С возможностью отказа	RR и V	RR/Ry и V	Необязательное	СКР
С обходным путем	RR и V	RR и V	СКР	СКР

[33] http://tools.ietf.org/html/draft-ietf-weirds-rdap-query-02

[34] Условные обозначения в таблице обзора моделей: RR — регистраторы, Ry — реестры, V — проверяющие

* **Примечание:** Модель, которая раньше называлась **«агрегированная СКР (АСКР)»**, была переименована в **«синхронизированную СКР (ССКР)»** для лучшего отражения особенности этой модели — единообразного и скоординированного использования данных, находящихся во многих местах. ВСЕ рассмотренные здесь модели надлежит внедрять с использованием передовых инженерных методов, чтобы добиться отказоустойчивости, высокой доступности и сбалансированности нагрузки, включая географически разнесенные центры обработки данных, надежные и многообразные возможности подключения и наличие инфраструктуры с резервированием в каждом центре обработки данных.

в. Рекомендуемая модель

Все перечисленные выше возможные модели системы отличаются друг от друга способом копирования или запроса регистрационных данных в СКР. ЭРГ тщательно изучила каждую модель, чтобы определить возможное влияние этих различий на разные свойства системы. Сравнив указанные возможные модели, ЭРГ пришла к выводу, что все они, кроме нынешней системы WHOIS, в той или иной степени могут соответствовать принципам СКР, рекомендованным ЭРГ. ЭРГ выбрала среди этих моделей для дальнейшего изучения две наиболее многообещающие — интегрированную модель и синхронизированную модель (ранее известную как «агрегированная модель») — **и в конечном итоге рекомендовала использовать синхронизированную модель (ССКР).**

Интегрированная модель (второе место)

Эта модель соответствует СКР, которая извлекает регистрационные данные из распределенных хранилищ, находящихся под управлением реестров с расширенным набором данных и проверяющих. При этом все они используют общую интегрированную схему данных. Данные не накапливаются в едином месте хранения, а вместо этого используется унифицированный открытый/регулируемый доступ через СКР к регистрационной информации, получаемой в режиме реального времени от всех реестров рДВУ (данные о доменных именах) и проверяющих (контактные данные).

В этой модели ИСКР извлекает данные из хранилищ проверяющих и регистраторов/реестров с использованием протокола RDAP. Поток контактных и регистрационных данных, соответствующий этой модели, подробнее рассмотрен в Приложении I (Блок-схемы процедур СКР) и проиллюстрирован на примере запросов в Приложении E.

Синхронизированная модель (ССКР) (рекомендуемая)

Эта модель соответствует СКР, которая в режиме близком к реальному времени копирует данные, полученные из распределенных хранилищ, находящихся под управлением реестров с расширенным набором данных и проверяющих, в синхронизированную систему, где эти данные накапливаются и хранятся с использованием распределенной архитектуры под управлением СКР.

В соответствии с этой моделью СКР является авторитетным источником данных, который предоставляет официальный доступ к ним, как описано выше.
В результате, СКР позволила бы отказаться от текущего требования САР (и текущей необходимости) о своевременном обновлении данных регистраторами и реестрами. Реестры, регистраторы и проверяющие могут предоставлять клиентам доступ к их собственным данным, однако ответы на все запросы защищенных данных должны быть получены из СКР. Эта модель учитывает предыдущие рекомендации относительно WHOIS и просьбы уменьшить путаницу для потребителей в плане места и процедуры доступа к регистрационным данным, а также сводит к минимуму издержки и требования к подотчетности для регистраторов и реестров.

Хотя доступ к данным предоставляет СКР, эти данные хранятся не в одном, а в нескольких местах, диверсифицированно и с резервированием в соответствии с передовыми инженерными методами для систем, которым необходима отказоустойчивость, высокая доступность и сбалансированность нагрузки. Реестры и проверяющие по-прежнему хранят собственные данные, однако СКР может использовать синхронизированные копии этих данных для более эффективной обработки запросов на получение доступа.

В этой модели проверяющие и регистраторы/реестры передают данные в ССКР с использованием протокола RDAP. Поток контактных и регистрационных данных, соответствующий этой модели, подробнее рассмотрен в Приложении I (Блок-схемы процедур СКР) и проиллюстрирован на примере запросов в Приложении E. Ниже сравниваются две модели, выбранные ЭРГ после применения методики, которая описана в Приложении F.

- **Последствия для безопасности** — обе эти модели дают похожие результаты при оценке последствий для безопасности. Хотя в комментариях общественности говорилось о том, что агрегированная (впоследствии переименованная в синхронизированную) модель, как она предложена в первоначальном отчете, создает риск из-за возникновения «единой точки отказа» в виде централизованного интерфейса, ЭРГ пришла к выводу, что этот риск не отличается от риска, который сегодня создают крупные реестры рДВУ и существующие в Интернете веб-сайты мирового масштаба. Современные передовые практические методы диктуют необходимость использования крупными информационными системами множества центров обработки данных, резервного хранилища и систем восстановления после аварий, а также географически диверсифицированной инфраструктуры с полным резервированием для снижения этих рисков.

  У синхронизированной модели есть дополнительное преимущество — возможность обеспечить большее единообразие при реализации мер безопасности и соблюдения политики. Благодаря надежному контролю над компонентами системы, синхронизированная модель с распределенной архитектурой, находящаяся под управлением одного оператора, скорее всего обеспечила бы боле унифицированный подход к достижению заявленных целей в области безопасности по сравнению с интегрированной моделью. Частично причиной этого является то, что в интегрированной модели потенциально тысячи реестров, регистраторов и проверяющих управляли бы соответствующими базами данных, имея различный уровень опыта и инвестиций в области практического обеспечения безопасности.

- **Вопросы юрисдикции и конфиденциальности** — обе эти модели дают похожие результаты при оценке последствий в плане юрисдикции и конфиденциальности. В интегрированной модели хранение данных и управление данными осуществляется на уровне реестров, при одновременном хранении дополнительных копий в других местах (а именно, у регистратора, проверяющего и в резервных центрах обработки данных, которые размещены

по всему миру). В синхронизированной модели хранение данных и управление данными осуществляется в нескольких местах, отдельно от реестров, при одновременном хранении дополнительных копий в других местах (у регистратора, реестра, проверяющего и в резервных центрах обработки данных, которые размещены по всему миру). При рассмотрении всех проанализированных моделей видно, что большинство из них не исключает передачу данных в несколько мест, кроме «модели с обходным путем», которая устраняет необходимость хранения контактных данных реестрами.

Более того, синхронизированная модель позволяет более последовательно применять правила соблюдения местных требований по защите конфиденциальности, поскольку в данном случае проще управлять этими правилами, администратором которых является единственный субъект (оператор синхронизированной СКР), а не больше тысячи потенциальных участников интегрированной модели.

- **Аккредитация** — применять требования аккредитации можно как в синхронизированной, так и в интегрированной модели. Обе модели способны предложить функции для отслеживания и предотвращения злоупотреблений в системе аккредитации, хотя, возможно, это проще сделать, когда база данных находится под управлением единственного субъекта, как в синхронизированной модели, по сравнению с более чем тысячей потенциальных участников интегрированной модели. Кроме того, реализация интегрированной модели потребовала бы дополнительных расходов, а также подробно сформулированных договорных обязательств, соглашений об уровне обслуживания и надзора со стороны отдела соблюдения договорных обязательств ICANN, необходимого для поддержки возможностей единообразного принуждения к соблюдению и аудита.

- **Функционирование** — синхронизированная модель предлагает действенные механизмы в ряде функциональных областей, которые сложнее получить в интегрированной модели. Например, создать дружелюбный к пользователю портал для отображения данных на нескольких языках и с использованием разных систем письменности, возможно, проще в синхронизированной модели, где можно было бы обеспечить более единообразный формат перевода и транслитерации контактных данных. Чтобы добиться аналогичного уровня единообразия в интегрированной модели, в соглашениях потребовалось бы четко сформулировать стандартные технические требования к переводу и транслитерации. Архитектура обеих моделей позволяет

предусмотреть выборочные проверки качества данных, хотя, скорее всего, их будет проще выполнить в синхронизированной модели.

Проблем, связанных с временем ожидания и синхронизацией при передаче данных, меньше в интегрированной модели, поскольку данные, которые необходимо отобразить, поступают непосредственно из реестра. Однако возникающие при извлечении данных в синхронизированной модели проблемы, связанные с временем ожидания, можно преодолеть, если проверяющие и регистраторы (через реестры) своевременно будут передавать в ССКР обновленные данные по протоколу EPP (см. принцип соблюдения обязательств № 108).

- **Реализация** — интегрированная модель лучше согласуется с распределенной моделью сегодняшней WHOIS, чем синхронизированная модель. Однако требования к рабочим характеристикам и возможностям поиска, необходимым для надежного предоставления рекомендованных ЭРГ функциональных возможностей, потребовали бы подробных спецификаций и показателей качества, намного превышающих те, которые предусмотрены в сегодняшней WHOIS. Потребовался бы больший надзор со стороны отдела соблюдения договорных обязательств ICANN и большие ресурсы для обеспечения того, чтобы все стороны в интегрированной системе функционировали на ожидаемом уровне. В рамках любой модели затрагиваемым участникам пришлось бы обновить свою платформу программного обеспечения для взаимодействия с интерфейсом СКР при передаче результатов поиска и необходимых контактных данных.

- **Затраты** — в синхронизированной модели возможно сокращение затрат регистраторов и реестров (а также проверяющих) благодаря устранению эксплуатационной нагрузки, вызванной необходимостью постоянно отвечать на сложные запросы через интерфейс СКР (например, на обратные запросы), что пришлось бы делать в интегрированной системе. В частности, сравнение затрат моделей (подробно описанное в Приложении F) позволило сделать следующие выводы:

  (1) При использовавшихся допущениях, основная часть СКР немного дешевле при использовании интегрированной модели СКР (ИСКР), чем при использовании синхронизированной модели СКР (ССКР). Однако интегрированная модель высокочувствительна к количеству обратных запросов. **При более высоком объеме обратных запросов ИСКР становится**

намного дороже ССКР. Например, при увеличении нагрузки со стороны обратных запросов с 1% до 3% модель ИСКР становится на 35% дороже модели ССКР. Если количество обратных запросов равно 5%, можно ожидать увеличения глобальных расходов на ИСКР приблизительно на 85%. Это важный фактор неопределенности и риска, связанный с моделью ИСКР. Предполагается, что модель ССКР менее чувствительна к количеству обратных запросов.

(2) Кроме того, **модель ИСКР сопряжена с большими затратами для всей экосистемы по причине ее [более высокой стоимости] для операторов реестров**. В модели ИСКР каждому оператору реестра пришлось бы реализовать и поддерживать — в соответствии с соглашениями SLA — ответы в режиме реального времени на запросы СКР по протоколу RDAP, в том числе на обратные запросы и запросы архивных данных WhoWas. Кроме того, для последней категории запросов оператору реестра пришлось бы хранить и обслуживать архивные данные, что привело бы к дополнительным издержкам реестров. Следует обратить внимание, что эти дополнительные затраты каждого реестра намного превысили бы последствия реализации основной части СКР, оценка которых дана выше.

(3) Кроме того, **модель ИСКР потребовала бы большего объема усилий по использованию приложений, поддержке, обслуживанию и тестированию** по сравнению с моделью ССКР, из-за ожидаемого большего объема взаимодействия с реестрами.

Более подробные сведения об анализе стоимости реализации моделей, рамках и методике этого анализа, а также об основных расчетных параметрах и допущениях можно найти в Приложении F и документе *«Анализ стоимости реализации моделей службы каталогов регистрации (СКР)*[35]», подготовленном для ICANN компанией IBM в марте 2014 года.

[35] https://community.icann.org/display/WG/EWG+Public+Research+Page

г. Принципы хранения, депонирования и регистрации данных

№ п/п	Общие требования к хранению, депонированию и регистрации данных
161.	Необходимо разработать политики размещения, сохранения, доступа и защиты конфиденциальности.
162.	Политики и способы реализации хранения, депонирования и регистрации должны соответствовать местному и международному законодательству.
	Принципы хранения
163.	Для сохранения избыточности систем и устранения единичной точки отказа данные должны находиться в нескольких местах (например, у проверяющего, регистратора, реестра, поставщика услуг депонирования и поставщика СКР).
164.	При наличии данных в нескольких местах необходимо поддерживать единообразие.
165.	СКР должна обрабатывать элементы данных безопасным образом, защищая конфиденциальность и целостность элементов данных, подвергающихся риску несанкционированного раскрытия или использования.
166.	Данные о транзакциях необходимо хранить в течение неопределенно долгого срока, чтобы поддерживать точную регистрацию их изменения с течением времени и обеспечить работоспособность функции WhoWas, но не дольше предельного обязательного срока (если таковой имеется), установленного применимыми законами о защите данных. Также нужно периодически удалять контактные данные, потерявшие свою актуальность, в соответствии с законами (например, через год после прекращения действия регистрации).
	Принципы депонирования[36]
167.	Следует проводить аудит данных, переданных на ответственное хранение, чтобы проверять формат, целостность и полноту депонированных данных.
168.	Депонирование и аудит депонирования проще координировать в модели синхронизированной СКР.
169.	Сами депонированные данные должны быть зашифрованы и непрозрачны для аудиторов.

[36] Депонированием называется создание в системе зашифрованной резервной копии данных и ее передача заслуживающей доверия третьей стороне (поставщику услуг депонирования) для целей восстановления в случае стихийного бедствия, системного сбоя и т. д. Для получения дополнительных сведений см. CAP.

170.	Депонированные данные должны храниться в течение такого срока, который соответствует требованиям Соглашения об аккредитации регистраторов, индивидуальных соглашений с реестрами рДВУ и применимых законов о защите данных. В настоящее время этим сроком будет длительность оплаченного субъектом периода опубликования данных и дополнительный период, равный двум годам после завершения оплаченного срока или более, если того требует Соглашение с реестром рДВУ, но не превышая максимального разрешенного законом срока.
	Принципы регистрации
171.	Запросы СКР должны регистрироваться в журналах как записи об использовании системы.
172.	Может потребоваться обобщение этих журналов для обнаружения злоупотреблений в распределенных системах.
173.	Изменения должны регистрироваться в журналах для создания архива элементов данных с течением времени.
174.	Доступ к оперативным журналам СКР должен быть ограничен кругом тех доверенных, прошедших проверку подлинности и авторизованных физических и юридических лиц, которые имеют особые цели и «должны это знать». Сюда необходимо включить уполномоченных операторов самой СКР (для подтверждения и устранения неисправностей в работе СКР) и лиц, уполномоченных обеспечивать защиту данных (для текущего контроля соответствия СКР законодательству о защите данных). (См. также раздел VIII(b) «Доступ правоохранительных органов».)

IX. Затраты и последствия

a. Принципы осуществления затрат

Как было отмечено в Приложении F, «Методика сравнения моделей», ЭРГ также рассмотрела затраты и последствия создания СКР. ЭРГ признает, что некоторые аспекты рекомендованной модели будут сопряжены с затратами, однако считает, что многие другие скрытые затраты, которые приходится нести в сегодняшней неэффективной и слишком часто неточной системой WHOIS, уменьшатся. Поскольку рекомендуемая СКР оказывает новые и улучшенные услуги, необходимо оценить как выгоды, так и издержки. Рекомендуемый подход впервые позволит органам, определяющим политику, разработать способы, позволяющие лицам, которые запрашивают регистрационные данные из системы, эффективно вносить вклад в работу этой системы.

Сегодняшние расходы на эксплуатацию WHOIS неизвестны, но подразумевают необходимость расходов для всей экосистемы, а не только для предлагающих услуги WHOIS реестров и регистраторов. Регистраторам нет необходимости выделять затраты на WHOIS, и у них могут возникнуть трудности при попытке различить расходы на предоставление таких услуг для рДВУ и для нДВУ. В результате неэффективности и недостатков сегодняшней WHOIS несут затраты другие участники экосистемы, например владельцы товарных знаков, которые оплачивают услуги компаний по защите фирменных наименований и коммерческие услуги WHOIS по выявлению кибersквоттеров.

ЭРГ рекомендует следующие принципы в отношении затрат:

№ п/п	Принципы осуществления затрат
175.	Не требующий проверки подлинности (нерегулируемый) доступ к открытым элементам данных должен предоставляться бесплатно.
176.	Требующий проверки подлинности (регулируемый) доступ правоохранительных органов к разрешенным элементам данных (при соблюдении надлежащей процедуры) может стать предметом особого рассмотрения в плане затрат.
177.	Структура СКР должна стремиться к экономической эффективности и минимизации затрат без ущерба для остальных целей.
178.	СКР следует управлять на основе модели возмещения издержек.
179.	Чтобы способствовать отказу от WHOIS, корпорация ICANN должна создать и профинансировать платформу разработки программного обеспечения СКР, чтобы минимизировать затраты на внедрение СКР реестрами/регистраторами, проверяющими и органами аккредитации пользователей СКР.
180.	Предоставление такой платформы разработки программного обеспечения не должно налагать чрезмерного бремени на пользователей СКР.

Если не углубляться в конкретные детали реализации, расходы можно распределить между участниками экосистемы. К примерам возможных способов возмещения затрат относится взимание разнообразных лицензионных сборов, в зависимости от пользователя, элементов данных, к которым получен доступ, или цели (таких как сборы за коммерческое использование, плата за подписку для пользователей, решающих ресурсоемкие задачи, или сборы за элитный доступ), или взимание платы за сопутствующие услуги (например, аттестационные сборы или плата за предварительную проверку).

СКР также может обеспечить экономию затрат для реестров и регистраторов, которые больше не должны предоставлять открытый доступ к данным или строго выполнять требования к уровню обслуживания в части быстродействия. Экономии затрат также можно добиться для инициаторов запросов, стремящихся получить данные, путем устранения неэффективности, причиной которой является несоблюдение требований поставщиками (регистраторами, реестрами, проверяющими или аккредитованными поставщиками услуг сохранения конфиденциальности/регистрации через доверенных лиц).

б. Преимущества по сравнению с текущей WHOIS, соответствующей CAP 2013

Недостатки WHOIS в течение последнего десятилетия были документально зафиксированы в многочисленных отчетах и исследованиях, которые перечислены в Приложении B. Улучшения системы WHOIS, которые отражены в Соглашении об аккредитации регистраторов 2013 года (CAP 2013), в сочетании с другими улучшениями, проистекающими из оценки Правлением ICANN рекомендаций группы проверки WHOIS, позволили устранить некоторые выявленные недостатки WHOIS.

Хотя CAP 2013 ввело несколько новых обязанностей, которые особо касаются требований к подтверждению и проверке для повышения точности, по-прежнему существуют другие серьезные недостатки. Эти недостатки перечислены ниже и сопоставлены с разделами настоящего отчета, где содержатся рекомендации по дальнейшим улучшениям.

Недостаток WHOIS, соответствующей CAP 2013	Устранение этого недостатка в СКР рассмотрено в разделе
Анонимный открытый доступ ко всем элементам данных создает среду, в которой возможен массовый сбор данных и злоупотребления с незначительной ответственностью или возможностью исправить ситуацию	III «Пользователи и цели» IV «Повышение подотчетности» VI(d) «Подотчетность и аудит»
Ограниченная возможность защиты конфиденциальности физических лиц	VI(a) «Защита данных» VII «Улучшение защиты конфиденциальности владельцев регистраций»

Недостаток WHOIS, соответствующей CAP 2013	Устранение этого недостатка в СКР рассмотрено в разделе
Ограниченные возможности обеспечения целостности регистрационных данных; владельцы регистраций без труда могут указать фальшивые контактные данные, в том числе принадлежащие другому лицу	V «Улучшение качества данных» V(g) «Право на уникальность контактных данных»
Отсутствие функций безопасности	IV(b) «Нерегулируемый и регулируемый доступ к данным» IV(c) «Аккредитация пользователей СКР»
Отсутствие возможностей аудита	VI(d) «Подотчетность и аудит» VIII(d) «Хранение, депонирование и регистрация данных»
Доступ не связан напрямую с заявленными законными целями	III «Пользователи и цели» III(e) «Целевые контактные лица»
Несогласованные интерфейсы запросов и ответы WHOIS	IV(b) «Нерегулируемый и регулируемый доступ к данным» VIII «Возможные модели СКР»
Отсутствие поддержки стандартов отображения интернационализированных регистрационных данных	IV(b) «Нерегулируемый и регулируемый доступ к данным» V(e) «Взаимодействие с проверяющими»
Ограниченная возможность применения различных правил для соблюдения разных правовых режимов защиты конфиденциальности данных	VI(a) «Защита данных»

Недостаток WHOIS, соответствующей CAP 2013	Устранение этого недостатка в СКР рассмотрено в разделе
Неприемлемые уровни точности являются источником неэффективности работы лиц, стремящихся установить связь с владельцами регистраций	V «Улучшение качества данных» III(e) «Целевые контактные лица»
Громоздкие процедуры управления обновлением контактных данных для нескольких доменных имен	V «Улучшение качества данных» V(c) «Процедура обеспечения точности, аудита и исправления нарушений»
Трудности при идентификации и установлении связи с клиентами служб сохранения конфиденциальности и регистрации через доверенных лиц	III(e) «Целевые контактные лица» VII(a) «Услуги сохранения конфиденциальности и регистрации через доверенных лиц» Приложение H «Модель передачи и раскрытия данных»
Отсутствие регулирования деятельности поставщиков услуг сохранения конфиденциальности и регистрации через доверенных лиц, кроме требований в CAP 2013, которые распространяются только на регистраторов и аффилированных с ними лиц	VII(a) «Услуги сохранения конфиденциальности и регистрации через доверенных лиц» Приложение H «Модель передачи и раскрытия данных»

в. Оценка рисков и анализ последствий

Как отмечалось в разделе IV «Улучшение подотчетности», ЭРГ рекомендует выполнить широкую оценку рисков с целью подтверждения того, что рекомендованные в настоящем документе принципы СКР действительно приведут к надлежащему сбору и раскрытию данных для определенных целей, обеспечивая правильное соотношение рисков и выгод.

14 марта ЭРГ предложила всем сторонам, которые предоставляют или используют регистрационные данные доменных имен рДВУ, принять участие в интерактивном опросе на тему рисков СКР, в том числе пользующимся сегодня данными WHOIS владельцам регистраций, регистраторам, реестрам и широкому спектру физических лиц, компаний и других организаций. Этот опрос позволил респондентам сообщить ЭРГ о рисках и выгодах, которые может им принести система следующего поколения, заменяющая WHOIS.

Перед окончательной доработкой настоящего отчета ЭРГ изучила зафиксированные благодаря этому опросу риски и выгоды, стремясь уменьшить непредвиденные и ненужные риски. По 29 мая 2014 года включительно на англоязычный вариант этого опроса поступило около 180 частичных ответов; приблизительно 100 респондентов ответили на все вопросы анкеты опроса. По состоянию на указанную дату состав респондентов был следующим: Северная Америка (68%), Европа (35%), Азия (20%), Латинская Америка (14%), Африка (11%) и Океания (10%); среди них было приблизительно равное количество тех, кто ИСПОЛЬЗУЕТ, и тех, кто ПРЕДОСТАВЛЯЕТ регистрационные данные. Ответы пролили свет на наиболее вероятные и значимые по силе воздействия риски и выгоды в следующих областях: техническая, функциональная, правовая и финансовая, безопасность и конфиденциальность. Приблизительно два десятка респондентов прокомментировали неизбежные и приемлемые риски и предложили способы передачи или снижения риска.

Чтобы обеспечить возможность участия широкого сообщества в рассмотрении данной темы, ЭРГ приняла решение оставить открытым опрос по рискам СКР до июля 2014 года включительно и опубликовать перевод анкеты опроса на другие языки. Ответы будут использоваться Правлением ICANN при анализе настоящего отчета, а также в качестве исходных данных будущего официального анализа затрат, рисков и выгод для всех заинтересованных сторон, которых может затронуть замена WHOIS на СКР[37].

[37] См. также объявление ICANN Общественное обсуждение оценки рисков DNS (1 этап)

X. Заключение и дальнейшие действия

После обсуждения перспектив для многих заинтересованных сторон экосистемы, опирающихся на регистрационные данные, ЭРГ единогласно рекомендует отказаться от сегодняшней модели WHOIS — предоставляющей каждому пользователю одинаковый анонимный доступ к регистрационным данным рДВУ — в пользу новой системы, созданной с нуля.

ЭРГ уверена, что рекомендованные в настоящем итоговом отчете принципы и СКР следующего поколения создают более прочный фундамент, чем тот, который существует сегодня, — фундамент, на основе которого можно защитить неприкосновенность личной жизни и обеспечить увеличение точности, подотчетности и прозрачности всей экосистемы ICANN на годы вперед. СКР опирается, но далеко выходит за рамки улучшений, внесенных в недавно согласованном САР 2013, как более полно описано в разделе IX(b).

Хотя итоговый отчет может показаться некоторым излишне подробным, он не является всеобъемлющим. Как отмечено в Приложении A, в настоящем отчете рассматривается каждый из заданных Правлением вопросов. Однако несколько проблем еще требуют более всестороннего рассмотрения в будущем — либо в рамках процесса разработки политики (ПРП), либо в рамках соответствующих усилий по реализации.

- **Органы аккредитации и политики для сообществ пользователей СКР.** Поскольку конкретные сообщества пользователей имеют право на доступ к защищенным данным для разрешенных целей, на этапе реализации необходимо сформировать политики идентификации полномочных членов этих сообществ, а также определить возможные органы аккредитации и модели, целесообразные для каждого сообщества.
- **Необходимые расширения протоколов EPP и RDAP.** Как подробно описано в Приложении G, ЭРГ рекомендует использовать для поддержки СКР стандартные протоколы, однако группа определила определенные расширения, которые потребуются для полноценной поддержки рекомендуемой модели СКР и элементов данных.
- **Оценка рисков и анализ последствий.** Как рассмотрено в разделе IX, ЭРГ рекомендует перед реализацией рекомендуемой СКР выполнить полную оценку рисков и анализ затрат и выгод, и уже начала проведение опроса с целью сбора необходимых для этого процесса данных.

- **Политика защиты конфиденциальности в СКР.** Как было рассмотрено в разделе VII, ЭРГ рекомендует сформулировать политику защиты конфиденциальности ICANN для СКР на основе стандартной передовой практики защиты конфиденциальности, а также разработать стандартные положения договоров, которые претворяли бы эту политику в жизнь во всей экосистеме СКР.
- **Перевод и транслитерация контактных данных.** Поскольку для решения этого вопроса в настоящее время идет процесс разработки политики (ПРП), ЭРГ приняла решение не дублировать усилия, ограничившись перечисленными в разделе IV(b) принципами, и вместо этого предлагает изучить в будущем результаты текущего ПРП с целью определения возможности применения любых новых политик в СКР.
- **Услуги сохранения конфиденциальности и регистрации через доверенных лиц.** Принципы ЭРГ, относящиеся к аккредитованным поставщикам услуг сохранения конфиденциальности и регистрации через доверенных лиц, потребуется рассмотреть в совокупности с выполняемой сейчас работой ОПРИ по решению этого вопроса, согласовав результат текущего ПРП с реализацией СКР.
- **Экосистема проверяющих.** Для создания программы аккредитации проверяющих и процедур проверки контактных данных владельцев регистраций и контактных лиц, находящихся в разных странах мира, потребуется дополнительное исследование на этапе реализации.

СКР отражает тщательно продуманные и сбалансированные компромиссы между взаимозависимыми компонентами, которые на следует разделять. В основе этих компромиссов лежат комментарии, полученные ЭРГ в ходе многочисленных общественных обсуждений, интернет-семинаров и консультаций, проведенных к настоящему времени. В результате, ЭРГ рекомендует Правлению направить настоящий итоговый отчет ОПРИ на утверждение в целом. Принятие решения о внедрении некоторых, но не всех этих принципов разработки СКР сведет на нет преимущества ее использования для всей экосистемы. У ЭРГ есть опасения, что изучение компонентов по отдельности может привести к противоречиям и тупиковым ситуациям в сообществе, которые сопровождали предыдущие попытки улучшения WHOIS.

ЭРГ передала настоящий итоговый отчет генеральному директору ICANN и Правлению, открыто опубликовала его в Интернете и проведет множество совещаний на лондонской конференции ICANN в июне 2014 года. Она также проведет интернет-семинары и предоставит другие возможности для обсуждения этого отчета и ответа на вопросы сообщества ICANN, касающиеся этого отчета. Настоящий итоговый отчет должен создать фундамент для процесса разработки

политики (ПРП) ОПРИ по запросу Правления в отношении предоставления регистрационных данных рДВУ и проведения в установленном порядке необходимых переговоров по условиям договоров. ЭРГ рекомендует при рассмотрении настоящего итогового отчета Правлением и сообществом ICANN выстраивать обсуждение на основе следующих вопросов:

- Является ли СКР более предпочтительной, чем сегодняшняя система WHOIS?
- Если нет, согласно ли сообщество ICANN с тем, что существующая система WHOIS должна продолжать работу и может удовлетворить потребности развивающегося мирового Интернета?

ЭРГ уверена, что настоящий итоговый отчет выполняет указание Правления ICANN содействовать переопределению цели и способов предоставления данных о регистрации рДВУ, и создаст фундамент, на котором сообщество ICANN (через ОПРИ) выработает новую глобальную политику в отношении справочных служб рДВУ.

ПРИЛОЖЕНИЕ A. ОТВЕТЫ НА ВОПРОСЫ ПРАВЛЕНИЯ

В резолюции Правления с указаниями относительно работы ЭРГ содержался ряд конкретных вопросов, на которые группа должна была дать ответы в процессе анализа. В настоящем приложении указаны разделы данного отчета, которые содержат сведения по интересующим Правление проблемам.

Вопросы и указания Правления	Разделы отчета
ЭРГ должна переопределить цели: • сбора, • сопровождения и • предоставления доступа к регистрационным данным рДВУ, и • обсудить средства защиты данных	Раздел III, «Пользователи и цели» Раздел VI, «Улучшение подотчетности»
Для чего необходим сбор данных?	Раздел III, «Пользователи и цели» Раздел VI(a), «Элементы данных»
Для каких целей будут использоваться данные?	Приложение D, «Цели и потребности в данных»
Кто собирает данные?	Раздел V, «Улучшение качества данных» Приложение I, «Блок-схемы процедур СКР»
Где и как долго хранятся данные?	Раздел VII, «Возможные модели СКР» Раздел VIII(d), «Хранение данных»
Где депонируются данные и на какой срок?	Раздел VIII(d), «Принципы хранения, депонирования и регистрации данных»
Кому и для чего необходимы эти данные?	Раздел III, «Пользователи и цели»
Кому и для чего необходим доступ к журналам доступа к данным?	Раздел VI(d), «Принципы подотчетности и аудита»
Открытый доступ к сведениям о регистрации доменного имени?	Раздел IV(b), «Нерегулируемый и регулируемый доступ к данным» Раздел VI(a), «Элементы данных» Раздел VII «Улучшение защиты конфиденциальности владельцев регистраций»
Доступ правоохранительных органов к сведениям о регистрации доменного имени?	Раздел III, «Пользователи и цели» Раздел VI(b), «Принципы доступа правоохранительных органов к данным»

Вопросы и указания Правления	Разделы отчета
Доступ владельцев интеллектуальной собственности к сведениям о регистрации доменного имени?	Раздел III, «Пользователи и цели»
Доступ специалистов по безопасности к сведениям о регистрации доменного имени?	Раздел III, «Пользователи и цели»
Что ценного получает общественность в результате доступа к регистрационным данным?	Раздел II(b), «Цель» Раздел III, «Пользователи и цели»
К каким из всех имеющихся регистрационных данных общественности нужен доступ?	Раздел VI(a), «Элементы данных»
Является ли протокол WHOIS лучшим выбором для предоставления этого доступа?	Раздел IV(b), «Нерегулируемый и регулируемый доступ к данным» Приложение G, «Возможность использования протоколов EPP и RDAP для поддержки СКР»
Безопасность	
Что входит в состав законных потребностей правоохранительных органов?	Раздел III, «Пользователи и цели» Раздел VI(b), «Принципы доступа правоохранительных органов к данным»
Как идентифицировать сотрудника правоохранительных органов?	Раздел IV(c), «Принципы аккредитации пользователей СКР» Раздел VI(b), «Принципы доступа правоохранительных органов к данным»
Какие регистрационные данные и с какой степенью точности позволяют установить реальную личность ответственной стороны?	Раздел V, «Улучшение качества данных» Раздел VI(a), «Элементы данных» Раздел VII(b), «Защищенные учетные данные»
Какие регистрационные данные и с какой степенью точности содержат ценную информацию для правоохранительных органов, стремящихся установить реальную личность ответственной стороны?	Раздел III, «Пользователи и цели» Приложение D, «Цели и потребности в данных»
Является ли протокол WHOIS лучшим выбором для обеспечения этого?	Раздел IV(b), «Нерегулируемый и регулируемый доступ к данным» Приложение G, «Возможность использования протоколов EPP и RDAP для поддержки СКР»

Вопросы и указания Правления	Разделы отчета
Владельцы интеллектуальной собственности	
Соответствует ли желаемый доступ к регистрационным данным доменных имен доступу, который есть у владельцев интеллектуальной собственности к аналогичным видам данных в других отраслях?	Раздел III, «Пользователи и цели» Раздел IV(c), «Принципы аккредитации пользователей СКР»
Как идентифицировать владельца интеллектуальной собственности?	Раздел IV(c), «Принципы аккредитации пользователей СКР»
К каким из всех имеющихся регистрационных данных владельцу интеллектуальной собственности нужен доступ?	Раздел III, «Пользователи и цели» Приложение D, «Цели и потребности в данных»
Какие регистрационные данные целесообразно сделать доступными?	Раздел VI(a), «Элементы данных»
Является ли протокол WHOIS целесообразным способом доступа?	Раздел IV(b), «Нерегулируемый и регулируемый доступ к данным» Приложение G, «Возможность использования протоколов EPP и RDAP для поддержки СКР»

ПРИЛОЖЕНИЕ B. ИССЛЕДОВАНИЯ С ЦЕЛЬЮ ОЦЕНКИ НЕДОСТАТКОВ WHOIS

- ККБС — отчет SAC 051
- ККБС — отчет SAC 054
- ККБС — отчет SAC 055
- Принципы ПКК для WHOIS
- Итоговый отчет группы проверки политики WHOIS
- Проект процедуры ICANN для разрешения конфликтов WHOIS с законодательством о неприкосновенности личной жизни
- Реестр требований к службе WHOIS — итоговый отчет
- Первоначальный отчет специальной рабочей группа по вопросам WHOIS 2 (2009 г.)
- Итоговый отчет специальной рабочей группа по вопросам службы WHOIS (2007 г.)
- Оценочное исследование решений для представления и отображения интернационализированных контактных данных
- Итоговый отчет ОПРИ о WHOIS с расширенным набором данных
- Промежуточный отчет ЭРГ по вопросам интернационализированных регистрационных данных
- Пересмотр процедуры ICANN для разрешения конфликтов WHOIS с законодательством о неприкосновенности личной жизни
- Проведенные ОПРИ исследования WHOIS, в том числе
    - Исследование точности контактной информации владельцев регистрации в WHOIS
    - Исследование распространенности доменных имен, зарегистрированных с использованием услуг сохранения конфиденциальности или доверенных лиц, в 5 крупнейших рДВУ
    - Исследование злоупотреблений в WHOIS

- Исследование вопросов идентификации владельцев регистраций в WHOIS
- Исследование злоупотреблений в WHOIS, связанных с услугами сохранения конфиденциальности и регистрации через доверенных лиц
- Опрос на тему осуществимости раскрытия и передачи данных WHOIS при регистрации через доверенных лиц/с сохранением конфиденциальности + приложения

ПРИЛОЖЕНИЕ C. ПРИМЕРЫ ВАРИАНТОВ ИСПОЛЬЗОВАНИЯ

Как описано в разделе III, ЭРГ проанализировала реальные примеры использования существующей системы WHOIS, чтобы выявить пользователей, желающих иметь доступ к регистрационным данным рДВУ, их цели, а также заинтересованные стороны и рассматриваемые данные. Перечень рассмотренных ЭРГ типичных примеров использования приведен ниже.

Цель	Примеры вариантов использования
Управление доменным именем	Создание учетной записи регистрации доменного имени
	Мониторинг изменения данных доменного имени
	Управление портфелем доменных имен
	Инициирование передачи доменного имени
	Удаление доменного имени
	Обновление данных DNS для доменного имени
	Продление регистрации доменного имени
	Подтверждение контактных данных доменного имени
Защита персональных данных	Связь с поставщиком услуг сохранения конфиденциальности/регистрации через доверенных лиц
	Связь с ответственным за утверждение защищенных учетных данных
Решение технических проблем	Связь с техническим персоналом доменного имени
Сертификация доменного имени	Выдача сертификатов доменных имен
Индивидуальное использование Интернета	Контакт с реальным миром
	Защита прав потребителей
Использование доменного имени в деловых целях Покупка или продажа	Посредническая продажа доменного имени
	Проверка охраноспособности товарного знака — доменного имени
	Приобретение доменного имени
	Запрос на покупку доменного имени
	История регистрации доменного имени
	Доменные имена определенного владельца регистраций
Исследование DNS в научных или общественных интересах	История регистрации доменного имени
	Доменные имена конкретного контактного лица
	Опрос владельца регистрации доменного имени или назначенного контактного лица

Цель	Примеры вариантов использования
Юридические действия	Контакт с пользователем доменного имени
	Борьба с мошенническим использованием данных владельцев регистраций
	История регистрации доменного имени
	Доменные имена конкретного контактного лица
Принуждение к соблюдению нормативных и договорных обязательств	Онлайновое налоговое расследование
	Разбирательства в рамках ЕПРД
	Выполнение договорных обязательств в экосистеме СКР
Расследование уголовных дел и предотвращение злоупотреблений в DNS	Проведение расследования в отношении неправомочного доменного имени
	Расследование преступной деятельности за рамками Интернета
	Услуги оценки репутации доменного имени
	Расследование преступной деятельности в Интернете
	Контактное лицо по вопросам злоупотреблений для взломанного доменного имени
Прозрачность DNS	Доступ общественности к регистрационным данным
Злонамеренная деятельность в Интернете	Перехват доменных имен
	Злонамеренная регистрация доменных имен
	Сбор регистрационных данных для спама/обмана

Таблица 7. Примеры вариантов использования

Чтобы проиллюстрировать методику ЭРГ, ниже приведен один пример использования. Дополнительные описания каждого примера использования, соответствующих пользователей СКР и потребностей в данных см. в разделе III.

Решение технических проблем — связь с техническим персоналом доменного имени

Цель/Сценарий № 1.

Кто-то столкнулся с эксплуатационной или технической проблемой, которая связана с зарегистрированным доменным именем. Он желает знать, с кем можно связаться для решения проблемы в режиме реального времени или близком к реальному времени, и поэтому использует СКР для определения соответствующего лица, специалиста или субъекта, способного решить данную проблему. Неполный перечень примеров технических проблем включает проблемы отправки и доставки электронной почты, проблемы разрешения в DNS, а также функциональные проблемы веб-сайтов.

Пример использования в кратком формате

Пример использования: определение лица, специалиста или субъекта, который может помочь в решении технической проблемы с доменным именем.

Основной сценарий использования: Пользователь получает доступ к СКР для извлечения контактных данных, связанных с зарегистрированными в одном или нескольких ДВУ доменными именами. Этот пользователь отправляет доменное имя в СКР на обработку. СКР возвращает информацию, связанную с указанным доменным именем и идентифицирующую лицо, специалиста или субъекта, к которому можно обратиться для решения технических проблем.

Пример использования в случайном формате

Наименование: определение лица, специалиста или субъекта, который может решить техническую проблему с доменным именем.

Основное действующее лицо: некто, столкнувшийся с технической проблемой, которая связана с зарегистрированным доменным именем.

Другие заинтересованные стороны: оператор СКР; связанное с зарегистрированным доменным именем лицо, специалист или субъект, который может решать технические проблемы; владелец регистрации (которому может быть интересна информация о проблемах эксплуатации); проверяющий (который мог выдать идентификатор контактного лица этому техническому специалисту); регистратор или поставщик услуг хостинга (который может выполнять эксплуатационное обслуживание); аккредитованный поставщик услуг сохранения конфиденциальности/регистрации через доверенных лиц (который может помочь в установлении связи с лицом, специалистом или субъектом, способным решать технические проблемы).

Рамки: взаимодействие с СКР

Уровень: задача пользователя

Элементы данных: в контексте этого примера использования наиболее полезны элементы данных, позволяющие общаться в режиме реального или почти реального времени. К ним относятся адрес электронной почты, адрес для передачи мгновенных сообщений, номер телефона и/или индикатор, который определяет указанный владельцем регистрации предпочтительный способ связи. В разделе 4 стандарта RFC 2142 содержится рекомендация по использованию адресов электронной почти вида abuse@, noc@, и security@ для «предоставления клиентам, поставщикам и другим лицам, испытывающим трудности с интернет-услугой организации, возможности обращаться за помощью», однако важно отметить, что открытый характер указанных адресов часто делает их привлекательной мишенью для лиц, занимающихся массовой рассылкой нежелательной почты.

Последовательность событий: Столкнувшееся с технической проблемой лицо (инициатор запроса) получает доступ к СКР для извлечения информации о доменных именах, зарегистрированных в одном или нескольких ДВУ. Доступ к СКР можно получить через веб-сайт или какие-то иные средства электронной обработки.

Этот инициатор отправляет запрос с указанием зарегистрированного доменного имени на обработку в систему.

СКР обрабатывает этот запрос и либо сообщает об ошибке с указанием ее причины, либо запрашивает регистрационные данные рДВУ для извлечения информации, связанной с лицом, специалистом или субъектом, который ранее был назначен в качестве ресурса для решения технических проблем с этим доменным именем.

СКР возвращает либо регистрационные данные, связанные с этим доменным именем, либо информацию об ошибке, возникшей при попытке извлечь данные.

Рис. 9. Пример использования

Приложение D. ЦЕЛИ И ПОТРЕБНОСТИ В ДАННЫХ

ЭРГ проанализировала примеры использования, чтобы выявить пользователей, желающих иметь доступ к регистрационным данным рДВУ, их цели, а также заинтересованные стороны и рассматриваемые данные. В приведенной ниже таблице обобщены элементы данных СКР, рекомендованные в разделе IV, и сопоставлены с разрешенными целями, которые определены в разделе III. Рекомендации по сбору и раскрытию каждого элемента данных см. в разделе IV.

Элемент данных	Цели
Доменное имя	Все
Серверы DNS	Управление доменным именем Решение технических проблем Сертификация доменного имени Покупка и продажа доменного имени в деловых целях Исследование DNS в научных или общественных интересах Принуждение к соблюдению нормативных и договорных обязательств Расследование уголовных дел и предотвращение злоупотреблений в DNS
Имя владельца регистрации и/или наименование организации Тип владельца регистрации Идентификатор контактного лица владельца регистрации Статус подтверждения контактного лица владельца регистрации Метка времени последнего обновления контактного лица владельца регистрации	Все
Идентификатор компании, являющейся владельцем регистрации	Управление доменным именем Сертификация доменного имени Индивидуальное использование Интернета Покупка и продажа доменного имени в деловых целях Юридические действия Исследование DNS в научных или общественных интересах Принуждение к соблюдению нормативных и договорных обязательств Расследование уголовных дел и предотвращение злоупотреблений в DNS Прозрачность DNS

Элемент данных	Цели
Почтовый адрес владельца регистрации, в том числе: Уличный адрес владельца регистрации Город владельца регистрации Регион/штат владельца регистрации Почтовый индекс владельца регистрации Страна владельца регистрации	Управление доменным именем Сертификация доменного имени Покупка и продажа доменного имени в деловых целях* Исследование DNS в научных или общественных интересах* Юридические действия* Принуждение к соблюдению нормативных и договорных обязательств Расследование уголовных дел и предотвращение злоупотреблений в DNS
Телефонный номер владельца регистрации + добавочный номер Альтернативный телефонный номер владельца регистрации + добавочный номер	Управление доменным именем Решение технических проблем Сертификация доменного имени Покупка и продажа доменного имени в деловых целях* Исследование DNS в научных или общественных интересах* Юридические действия* Принуждение к соблюдению нормативных и договорных обязательств Расследование уголовных дел и предотвращение злоупотреблений в DNS
Адрес электронной почты владельца регистрации Альтернативный адрес электронной почты владельца регистрации	Все
Номер факса владельца регистрации + добавочный номер	Управление доменным именем Сертификация доменного имени Покупка и продажа доменного имени в деловых целях* Исследование DNS в научных или общественных интересах* Юридические действия* Принуждение к соблюдению нормативных и договорных обязательств
Новые способы связи с владельцем регистрации, сведения о которых могут быть опубликованы по его желанию: Данные для отправки владельцу регистрации SMS Данные для отправки владельцу регистрации мгновенных сообщений Идентификатор владельца регистрации в социальной сети Альтернативный идентификатор владельца регистрации в социальной сети URL-адрес контактного лица владельца регистрации URL-адрес владельца регистрации по вопросам злоупотреблений	Может принести пользу для любой разрешенной цели как альтернатива адресу электронной почты владельца регистрации

Элемент данных	Цели
Идентификатор контактного лица по административным вопросам Элементы контактных данных администратора	Управление доменным именем Сертификация доменного имени Покупка и продажа доменного имени в деловых целях Исследование DNS в научных или общественных интересах Прозрачность DNS
Идентификатор контактного лица по правовым вопросам Элементы контактных данных специалиста по правовым вопросам	Управление доменным именем Сертификация доменного имени Исследование DNS в научных или общественных интересах Юридические действия Принуждение к соблюдению нормативных и договорных обязательств Прозрачность DNS
Идентификатор контактного лица по техническим вопросам Элементы контактных данных технического специалиста	Управление доменным именем Решение технических проблем Сертификация доменного имени Исследование DNS в научных или общественных интересах Прозрачность DNS
Идентификатор контактного лица по вопросам злоупотреблений Элементы контактных данных специалиста по вопросам злоупотреблений	Управление доменным именем Сертификация доменного имени Исследование DNS в научных или общественных интересах Расследование уголовных дел и предотвращение злоупотреблений в DNS Прозрачность DNS
Идентификатор контактного лица по вопросам сохранения конфиденциальности/регистрации через доверенных лиц Элементы контактных данных специалиста по вопросам сохранения конфиденциальности/регистрации через доверенных лиц	Управление доменным именем Защита персональных данных Сертификация доменного имени Исследование DNS в научных или общественных интересах Прозрачность DNS
Идентификатор контактного лица по коммерческим вопросам Элементы контактных данных специалиста по коммерческим вопросам	Управление доменным именем Сертификация доменного имени Индивидуальное использование Интернета Исследование DNS в научных или общественных интересах Прозрачность DNS
Делегирование DNSSEC	Управление доменным именем Исследование DNS в научных или общественных интересах

Элемент данных	Цели
Состояние регистрации Состояние на стороне клиента (регистратор) Состояние на стороне сервера (реестр)	Управление доменным именем Покупка и продажа доменного имени в деловых целях Исследование DNS в научных или общественных интересах Принуждение к соблюдению нормативных и договорных обязательств Расследование уголовных дел и предотвращение злоупотреблений в DNS
Регистратор Реселлер URL-адрес регистратора Идентификатор IANA регистратора Адрес электронной почты контактного лица регистратора по вопросам злоупотреблений Номер телефона контактного лица регистратора по вопросам злоупотреблений URL-адрес сайта Internic для отправки жалоб	Управление доменным именем Покупка и продажа доменного имени в деловых целях Исследование DNS в научных или общественных интересах Принуждение к соблюдению нормативных и договорных обязательств Расследование уголовных дел и предотвращение злоупотреблений в DNS Прозрачность DNS
Юрисдикция регистратора Юрисдикция реестра Язык соглашения о регистрации	Все
Дата первоначальной регистрации	Управление доменным именем Покупка и продажа доменного имени в деловых целях Исследование DNS в научных или общественных интересах Принуждение к соблюдению нормативных и договорных обязательств
Дата создания Дата обновления Дата истечения срока действия регистрации	Управление доменным именем Покупка и продажа доменного имени в деловых целях Исследование DNS в научных или общественных интересах Принуждение к соблюдению нормативных и договорных обязательств Расследование уголовных дел и предотвращение злоупотреблений в DNS

Примечание: Для доступа к защищенным элементам данных владельца регистрации, который иногда необходим для целей, отмеченных выше *, может потребоваться подтверждение необходимости знать эту информацию; см. раздел III, где рассматриваются «Разрешенные закрытые данные».

ПРИЛОЖЕНИЕ E. ПРИМЕРЫ ДОСТУПА С ПРОВЕРКОЙ И БЕЗ ПРОВЕРКИ ПОДЛИННОСТИ

В приведенной ниже записи регистрационных данных пример WHOIS, соответствующей CAP 2013, расширен для отражения рекомендованных ЭРГ принципов сбора и раскрытия данных.

Элементы, выделенные серым цветом, не обязательны для сбора; остальные являются обязательными.

Выделенные полужирным шрифтом элементы всегда являются общедоступными; остальные могут быть защищены по выбору владельца регистрации или владельца контактных данных.

Состояние регистрации: x **Делегирование DNSSEC: signedDelegation** **Состояние на стороне клиента: DeleteProhibited (удаление запрещено), RenewProhibited (обновление запрещено), TransferProhibited (передача запрещена)** **Состояние на стороне сервера: DeleteProhibited (удаление запрещено), RenewProhibited (обновление запрещено), TransferProhibited (передача запрещена)** **Регистратор: ПРИМЕР КОМПАНИИ РЕГИСТРАТОРА** **Реселлер: ПРИМЕР РЕСЕЛЛЕРА** **Юрисдикция регистратора: ПРИМЕР ЮРИСДИКЦИИ** **Юрисдикция реестра: ПРИМЕР ЮРИСДИКЦИИ** **Язык соглашения о регистрации: АНГЛИЙСКИЙ** **Дата создания: 2000-10-08T00:45:00Z** **Дата первоначальной регистрации: 2000-10-08T00:45:00Z** **Дата истечения срока действия регистрации: 2010-10-08T00:44:59Z** **Дата обновления: 2009-05-29T20:13:00Z** **URL-адрес регистратора: http://www.example-registrar.tld** **Идентификатор IANA регистратора: 5555555** **Адрес эл. почты для связи с регистратором по вопросам злоупотреблений: email@registrar.tld** **Номер телефона для связи с регистратором по вопросам злоупотреблений: +1.1235551234** **URL-адрес сайта Internic для отправки жалоб: http://wdprs.internic.net/**	Данные предоставляет реестр или регистратор

Доменное имя: EXAMPLE.TLD **Сервер имен: NS01.EXAMPLE-REGISTRAR.TLD** Имя владельца регистрации: ПРИМЕР ВЛАДЕЛЬЦА РЕГИСТРАЦИИ **Тип владельца регистрации: ЮРИДИЧЕСКОЕ ЛИЦО** **Идентификатор контактного лица владельца регистрации: xxxx-xxxx** (выдается аккредитованным СКР проверяющим) **Статус подтверждения контактного лица владельца регистрации (от проверяющего)** **Метка времени последнего подтверждения контактного лица владельца регистрации (от проверяющего)**	Получено от владельца регистрации
Организация владельца регистрации: ПРИМЕР ОРГАНИЗАЦИИ Идентификатор компании, являющейся владельцем регистрации: D-U-N-S #12345 (выдается компанией Dunn and Bradstreet)	
Адрес электронной почты владельца регистрации: EMAIL@EXAMPLE.TLD	
Альтернативный адрес электронной почты владельца регистрации: EXAMPLE@OTHERDN.TLD	
Улица владельца регистрации: ПРИМЕР УЛИЦЫ 123 Город владельца регистрации: ЛЮБОЙ ГОРОД	
Регион владельца регистрации: ЛР Почтовый индекс владельца регистрации: A1A1A1	
Страна владельца регистрации: AA Тел. владельца регистрации: +1.5555551212 Доб. телефонный номер владельца регистрации: 1234	
Альтернативный телефонный номер владельца регистрации: <номер мобильного телефона> Доб. альтернативный телефонный номер владельца регистрации: 1234 Факс владельца регистрации: +1.5555551213 Доб. номер факса владельца регистрации: 4321 Данные для отправки владельцу регистрации SMS: <номер для SMS-сообщений> Данные для отправки владельцу регистрации мгновенных сообщений: <маркер MC> Идентификатор владельца регистрации в социальной сети: <маркер CC> Альтернативный идентификатор владельца регистрации в социальной сети: <другой маркер CC> URL-адрес контактного лица владельца регистрации: <ссылка на форму или инструкции для связи> URL-адрес контактного лица владельца регистрации: <ссылка на форму или инструкции для сообщения о нарушениях>	

Идентификатор контактного лица по административным вопросам: xxxx-xxxx (за которым следуют контактные данные ЦКЛ по административным вопросам*)	Владелец регистрации обязан публиковать данные о целевых контактных лицах для обязательных типов ЦКЛ
Идентификатор контактного лица по техническим вопросам: xxxx-xxxx (за которым следуют контактные данные ЦКЛ по техническим вопросам*)	
Идентификатор контактного лица по правовым вопросам: xxxx-xxxx (за которым следуют контактные данные ЦКЛ по правовым вопросам*)	
Идентификатор контактного лица по вопросам злоупотреблений: xxxx-xxxx (за которым следуют контактные данные ЦКЛ по вопросам злоупотреблений*)	
Идентификатор контактного лица по коммерческим вопросам: xxxx-xxxx (только в том случае, если тип владельца регистрации = юридическое лицо) (за которым следуют контактные данные ЦКЛ по коммерческим вопросам*)	
Идентификатор контактного лица поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц: xxxx-xxxx (только в том случае, если тип владельца регистрации = поставщик услуг сохранения конфиденциальности/регистрации через доверенных лиц) (за которым следуют контактные данные ЦКЛ поставщика услуг КД*)	

Ключ: Элементы, выделенные серым цветом, не обязательны для сбора или подлежат сбору в определенных ситуациях; остальные являются обязательными. Выделенные полужирным шрифтом элементы всегда являются общедоступными; остальные могут быть защищены по выбору владельца регистрации или владельца контактных данных. * Элементы данных ЦКЛ проиллюстрированы здесь неполностью.

Пример № 1. Запрос открытых данных без проверки подлинности для решения технической проблемы

1) Пользователь отправляет в СКР запрос без проверки подлинности (ДИ = MerchantZ.gtld, цель = решение технической проблемы, данные = все)

2) СКР оценивает запрос:
   Без проверки подлинности, поскольку этот запрос не прошел проверку подлинности
   Без авторизации пользователя, то есть предоставляется доступ к общедоступным данным
   Доступ ограничивается общедоступными данными, необходимыми для решения технической проблемы, — то есть передаются все запрошенные общедоступные данные для этого доменного имени ПЛЮС данные контактного лица по техническим вопросам

3) СКР извлекает запрашиваемые элементы данных:
   Данные MerchantZ.gtld извлекаются из кэша СКР (в синхронизированной модели) или реестра (в интегрированной модели) с передачей только общедоступных элементов данных, определенных для этой цели, в том числе следующих
   Идентификатор контактного лица владельца регистрации = 12345
   Тип владельца регистрации = Юридическое лицо
   Организация владельца регистрации = MerchantZ, Inc.[38]
   Идентификатор контактного лица по техническим вопросам = 67890

   Идентификатор контактного лица по техническим вопросам [67890] извлекается из кэша СКР или проверяющего, с получением только общедоступных элементов данных, опубликованных этим контактным лицом специально для указанной цели, в том числе следующих
   Идентификатор ЦКЛ = 67890

   Имя ЦКЛ = <*имя субъекта, ответственного за решение технических проблем с доменным именем MerchantZ.gtld*>

[38] Данные об организации владельца регистрации предоставляют те владельцы регистраций, у которых в качестве типа владельца регистрации выбрано «Юридическое лицо» или «Аккредитованный поставщик услуг сохранения конфиденциальности/регистрации через доверенных лиц»; эти данные могут отсутствовать, когда типом владельца регистрации является используемое по умолчанию значение «Не указан»

Адрес электронной почты ЦКЛ = <*обязательный адрес электронной почты субъекта, ответственного за решение технических проблем с доменным именем MerchantZ.gtld*>

Альтернативный адрес электронной почты ЦКЛ = <*рекомендуемый альтернативный адрес электронной почты субъекта, ответственного за решение технических проблем с этим ДИ*>

Номер телефона ЦКЛ = <*рекомендуемый номер телефона субъекта, ответственного за решение технических проблем с* этим ДИ>

URL-адрес ЦКЛ = <*рекомендуемая ссылка для контакта, опубликованная субъектом, ответственным за решение технических проблем с этим ДИ*>

<*любые необязательные общедоступные элементы данных, опубликованные этим субъектом*>

4) СКР возвращает пользователю сообщение об ошибке или успешно полученный ответ. Например:

Доменное имя: MerchantZ.gtld
Состояние регистрации: x
Состояние на стороне клиента: DeleteProhibited (удаление запрещено), RenewProhibited (обновление запрещено), TransferProhibited (передача запрещена)
Состояние на стороне сервера: DeleteProhibited (удаление запрещено), RenewProhibited (обновление запрещено), TransferProhibited (передача запрещена)
Регистратор: EXAMPLE REGISTRAR LLC
Юрисдикция регистратора: ПРИМЕР ЮРИСДИКЦИИ
Юрисдикция реестра: ПРИМЕР ЮРИСДИКЦИИ
Язык соглашения о регистрации: АНГЛИЙСКИЙ
Дата создания: 2000-10-08T00:45:00Z
Дата истечения срока действия регистрации: 2010-10-08T00:44:59Z
Дата обновления: 2009-05-29T20:13:00Z
URL-адрес регистратора: http://www.example-registrar.tld
Идентификатор IANA регистратора: 5555555
Адрес электронной почты контактного лица регистратора по вопросам злоупотреблений: email@registrar.tld
Номер телефона контактного лица регистратора по вопросам злоупотреблений: +1.1235551234
URL-адрес сайта Internic для отправки жалоб:http://wdprs.internic.net/

Сервер имен: NS01.EXAMPLE-REGISTRAR.TLD *Идентификатор контактного лица владельца регистрации = 12345* *Тип владельца регистрации = Юридическое лицо* *Организация владельца регистрации = MerchantZ, Inc.* *Адрес электронной почты владельца регистрации = 12345@MerchantZ.gtld* *Статус подтверждения контактного лица владельца регистрации = Функционально-проверен* *Метка времени последнего подтверждения контактного лица владельца регистрации = x* *<Прочие необязательные общедоступные элементы данных, опубликованные владельцем регистрации для этого ДИ>*
Идентификатор техн. контакта = 67890 *Идентификатор ЦКЛ = 67890* *Статус подтверждения ЦКЛ = Функционально-проверен* *Метка времени последнего подтверждения ЦКЛ = x* *Имя ЦКЛ: ПРИМЕР ТЕХНИЧЕСКОГО СПЕЦИАЛИСТА* *Адрес электронной почты ЦКЛ = 67890@SuperbHostingServices.gtld* *Альтернативный адрес электронной почты ЦКЛ = SuperbHostingServices@OtherDN.gtld* *Номер телефона ЦКЛ =+1.1235567890* *URL-адрес ЦКЛ=TechSupport@SuperbHostingServices.gtld* *<Необязательные общедоступные элементы данных, опубликованные этим ЦКЛ>*

Пример № 2. Запрос защищенных данных с проверкой подлинности для решения технической проблемы

1) Пользователь отправляет в СКР запрос с проверкой подлинности (ДИ = PersonY.gtld, цель = решение технической проблемы, данные = все)

2) СКР оценивает запрос:
   - Если «А» прошел проверку подлинности, одобряется запрос на получение защищенных данных
   - Если «А» — аккредитованный интернет-провайдер, предоставляется доступ к контактным данным для решения технических проблем
   - Доступ ограничивается общедоступными+защищенными данными, необходимыми для решения технической проблемы
   - Доступ ограничивается общедоступными+защищенными данными, необходимыми для решения технической проблемы, — то есть всеми запрошенными общедоступными+защищенными данными для этой цели ПЛЮС данные контактного лица по техническим вопросам

3) СКР извлекает запрашиваемые элементы данных:
   Данные PersonY.gtld извлекаются из кэша СКР (в синхронизированной модели) или реестра (в интегрированной модели) с получением только общедоступных+защищенных элементов данных, определенных для этой цели, в том числе следующих:

   Идентификатор контактного лица владельца регистрации = 12345
   Тип владельца регистрации = Не указан
   <любые необязательные общедоступные или защищенные элементы данных, опубликованные этим владельцем регистрации — например, если владелец регистрации примет такое решение, его или ее имя>
   Идентификатор контактного лица по техническим вопросам = 67890[39]

   Идентификатор контактного лица по техническим вопросам [67890] извлекается из кэша СКР или проверяющего, с получением только общедоступных + защищенных элементов данных, опубликованных этим контактным лицом специально для указанной цели, в том числе следующих

[39] Если во время регистрации ДИ владелец регистрации не указывает никаких идентификаторов контактных лиц, его следует проинформировать о том, что в качестве основного ЦКЛ будет опубликовано его собственное имя и адрес, и дать возможность выразить согласие, указать другой идентификатор основного ЦКЛ (например, идентификатор контактного лица поставщика услуг регистрации через доверенных лиц) или отменить регистрацию.

Идентификатор ЦКЛ = 67890

Адрес электронной почты ЦКЛ = <*обязательный адрес электронной почты субъекта, ответственного за решение технических проблем с доменным именем PersonY.gtld*>

Альтернативный адрес электронной почты ЦКЛ = <*рекомендуемый альтернативный адрес электронной почты субъекта, ответственного за решение технических проблем с этим ДИ*>

Номер телефона ЦКЛ = <*рекомендуемый номер телефона субъекта, ответственного за решение технических проблем с* этим ДИ>

URL-адрес ЦКЛ = <*рекомендуемая ссылка для контакта, опубликованная субъектом, ответственным за решение технических проблем с этим ДИ*>

<*любые необязательные общедоступные или защищенные элементы данных, опубликованные этим субъектом — например, номер для отправки SMS*>

4) СКР возвращает пользователю сообщение об ошибке или успешно полученный ответ. Например:

Доменное имя: PersonY.gtld
Состояние регистрации: x
Состояние на стороне клиента: DeleteProhibited (удаление запрещено), RenewProhibited (обновление запрещено), TransferProhibited (передача запрещена)
Состояние на стороне сервера: DeleteProhibited (удаление запрещено), RenewProhibited (обновление запрещено), TransferProhibited (передача запрещена)
Регистратор: EXAMPLE REGISTRAR LLC
Юрисдикция регистратора: ПРИМЕР ЮРИСДИКЦИИ
Юрисдикция реестра: ПРИМЕР ЮРИСДИКЦИИ
Язык соглашения о регистрации: АНГЛИЙСКИЙ
Дата создания: 2000-10-08T00:45:00Z
Дата истечения срока действия регистрации: 2010-10-08T00:44:59Z
Дата обновления: 2009-05-29T20:13:00Z
URL-адрес регистратора: http://www.example-registrar.tld
Идентификатор IANA регистратора: 5555555
Адрес электронной почты контактного лица регистратора по вопросам злоупотреблений: email@registrar.tld
Номер телефона контактного лица регистратора по вопросам злоупотреблений: +1.1235551234
URL-адрес сайта Internic для отправки жалоб:http://wdprs.internic.net/

Сервер имен: NS01.EXAMPLE-REGISTRAR.TLD *Идентификатор контактного лица владельца регистрации = 12345* *Тип владельца регистрации = Не указан* *Адрес электронной почты владельца регистрации = 12345@PersonY.gtld* *Статус подтверждения контактного лица владельца регистрации = Функционально-проверен* *Метка времени последнего подтверждения контактного лица владельца регистрации =x* *<Прочие необязательные общедоступные или защищенные элементы данных, опубликованные владельцем регистрации для этого ДИ, например имя владельца регистрации, номер владельца регистрации для SMS или URL-адрес контактного лица владельца регистрации>*
Идентификатор техн. контакта = 67890 *Идентификатор ЦКЛ = 67890* *Статус подтверждения ЦКЛ = Функционально-проверен* *Метка времени последнего подтверждения ЦКЛ = x* *Имя ЦКЛ: ПРИМЕР ТЕХНИЧЕСКОГО СПЕЦИАЛИСТА* *Адрес электронной почты ЦКЛ = 67890@SuperbHostingServices.gtld* *Альтернативный адрес электронной почты ЦКЛ = SuperbHostingServices@OtherDN.gtld* *Номер телефона ЦКЛ =+1.1235567890* *URL-адрес ЦКЛ=TechSupport@SuperbHostingServices.gtld* *<Необязательные общедоступные или защищенные элементы данных, опубликованные этим ЦКЛ>*

Пример № 3. Запросы на получение разрешенных закрытых данных для покупки/продажи доменных имен или юридических действий

Ниже проиллюстрировано расследование возможного нарушения прав на товарный знак, однако аналогичные отправные моменты и этапы относятся к покупке доменных имен, слиянию и приобретению активов, и ко многим другим расследованиям для этих и других целей.

Этап 1) Пользователь СКР входит в систему органа аккредитации (определение которого дано в разделе IV(c), «Аккредитация пользователей СКР») и заверяет не только в том, что его целью является юридическое действие, но и в том, что полученные данные будут использованы для расследования возможного нарушения прав на товарный знак субъектом «X». Пользователь указывает имя и контактные данные физического/юридического лица, которое является интересующим его субъектом. Таким образом, запросы к СКР для этой цели будут по определению ограничены регистрационными данными, связанными с этим субъектом.

Этап 2) Теперь пользователь СКР может выполнить обратный запрос по значениям, уже известным об этом субъекте, выполняя поиск в СКР списка доменных имен, содержащих следующие заданные значения:

- Имя/организация владельца регистрации и/или ЦКЛ
- Телефон/альтернативный телефон владельца регистрации и/или ЦКЛ
- Почтовый адрес владельца регистрации и/или ЦКЛ
- Адрес эл. почты/альтернативный адрес эл. почты владельца регистрации и/или ЦКЛ

Некоторые из таких этих элементов данных могут быть защищены. Выполняется обратный запрос с целью поиска этих разрешенных закрытых данных, но только для указанного значения и заявленной цели, которые были подробно описаны на этапе аттестации.

Этап 3) Получив список доменных имен, которые могут использоваться для расследуемого нарушения прав на товарный знак, пользователь СКР теперь может отправлять в СКР запросы по доменным именам для получения данных, которые необходимы при оценке обстоятельств, а именно:

- Идентификатор контактного лица
- Даты регистрации
- Юрисдикция регистратора
- Юрисдикция реестра
- Страна владельца регистрации (юрисдикция владельца регистрации)
- Организация владельца регистрации и
- Идентификатор компании, являющейся владельцем регистрации

Та же самая информация по этим доменным именам может быть запрошена с использованием запросов WhoWas. На этом этапе все элементы данных, кроме одного, общедоступны; единственным защищенным элементом является страна владельца регистрации.

Этап 4) Сделав вывод о целесообразности дальнейших действий, пользователь СКР может выполнить в системе запрос для извлечения опубликованного общедоступного идентификатора контактного лица по правовым вопросам и соответствующих контактных данных (включая имя/организацию, номер телефона и почтовый адрес этого ЦКЛ). Эти результаты могут использоваться для попытки установить связь с назначенным владельцем регистрации контактным лицом по

правовым вопросам или для возбуждения иска, подачи жалобы в рамках ЕПРД или иного юридического действия.

Этап 5) Если контактное лицо по правовым вопросам не признает ответственности за доменное имя, для юридического действия могут потребоваться все контактные данные владельца регистрации. Значительная часть этих данных могла быть уже известна на этапе 1 и получена не из СКР. Однако могут существовать определенные пробелы, которые следует заполнить на данном этапе.

Данный пример иллюстрирует взаимодействие с СКР, которое может предусматривать расследования и возможные юридические действия в связи с нарушением прав на товарные знаки. Однако весьма похожая последовательность этапов может наблюдаться для других видов юридических действий, а также при изучении активов в виде доменных имен во время их покупки/продажи. В ситуациях, которые предусматривают получение защищенных данных, орган аккредитации должен нести ответственность за аудит доступа, чтобы обнаружить запросы, выходящие за рамки заявленных узких рамок, и принять меры по предотвращению злоупотреблений и обеспечению соблюдения условий и положений. Наличие аттестации пользователей СКР поможет органу аккредитации выполнить аудит доступа и расследовать возможные злоупотребления. Это также будет фактором, препятствующим сбору компрометирующих материалов.

ПРИЛОЖЕНИЕ F. РАССМОТРЕННЫЕ МОДЕЛИ И МЕТОДЫ ПОСТРОЕНИЯ СИСТЕМ

Помимо моделей, описанных ранее в разделе Возможные модели СКР, ЭРГ рассмотрела следующие альтернативы, однако признала каждую из них менее жизнеспособной, чем интегрированная или синхронизированная модель, по причинам, которые обобщены ниже.

Существующая WHOIS

Эта модель описывает полностью распределенный и автономный подход, который используется в сегодняшней системе WHOIS, где каждый реестр и регистратор предлагает собственные услуги WHOIS без их интеграции в масштабе всех рДВУ. Хотя можно создать централизованный портал, чтобы обеспечить доступ к службам WHOIS всех рДВУ, каждый реестр будет по-прежнему предоставлять свое собственное хранилище, управление которым осуществляется автономно, и доступ либо прямой (для расширенного набора данных), либо через делегирование регистраторам (минимальный набор данных).

Региональная модель

Эта модель соответствует СКР, которая периодически копирует данные из распределенных хранилищ, находящихся под управлением реестров и проверяющих, в региональные хранилища, расположенные в разных странах мира. Реестры и проверяющие по-прежнему хранят данные, однако СКР может использовать региональные копии этих данных для более эффективной обработки запросов на получение доступа. Региональные хранилища находятся под управлением СКР, однако подчиняются законам той юрисдикции, где они размещены.

Модель с возможностью отказа

Эта модель соответствует СКР, которая периодически копирует данные из распределенных хранилищ, находящихся под управлением реестров, в синхронизированное хранилище, находящееся под управлением СКР. В этой модели реестр может отказаться от использования синхронизированного хранилища, если согласится предоставить инфраструктуру, необходимую для обработки существенного количества запросов в соответствии с соглашениями об уровне обслуживания (SLA) в плане доступности и рабочих характеристик.

Модель с обходным путем

Эта модель соответствует СКР, которая периодически копирует данные из распределенных хранилищ, находящихся под управлением регистраторов, в синхронизированное хранилище, находящееся под управлением СКР. Согласно этой модели, реестры исключаются из списка источников регистрационных данных; вместо этого для ответов на запросы к СКР используются синхронизированные регистрационные данные, скопированные непосредственно из заслуживающих доверия источников.

Методика, которая использовалась для сравнения моделей системы

ЭРГ рассмотрела сопутствующие затраты и уязвимости с точки зрения безопасности, присущие нынешней системе WHOIS, многие из которых рассмотрены в отчетах, перечисленных в Приложении B и подтверждающих недостатки WHOIS. Было выполнено сравнение и сопоставление затрат и уязвимостей существующей системы WHOIS и возможных моделей. Кроме того, ЭРГ сравнила плюсы и минусы каждой из возможных моделей, используя для этого следующие критерии:

Последствия для безопасности

- **Единая точка отказа:** принимая во внимание использование распределенной архитектуры и основного поставщика услуг, насколько уязвима данная модель при отказе любой отдельно взятой системы? Станет ли отказ какой-либо отдельно взятой системы причиной недоступности всей или некоторой регистрационной информации? **Примечание:** следует использовать проверенные практические методы проектирования баз данных и управления ими, чтобы обеспечить внутреннюю избыточность и резервное копирование данных, которые действительно необходимы для обеспечения доступности данных в период отказа.
- **Подверженность внутренним злоупотреблениям:** Насколько уязвима модель для внутренних злоупотреблений вследствие доступа администратора/ оператора к регистрационной информации, которая хранится или проходит через какую-то систему, входящую в состав модели? Могут ли внутренние злоупотребления сделать возможным несанкционированный доступ ко всем данным или их части? Насколько легко можно было бы внедрить средства контроля для обнаружения/предотвращения внутренних злоупотреблений?
- **Подверженность внешним атакам:** Насколько уязвима модель для внешних атак на какую-то систему, входящую в состав модели? Могут ли внешние атаки сделать возможным нарушение конфиденциальности всех владельцев регистраций или их части? Насколько легко можно было бы внедрить средства контроля для обнаружения/предотвращения внешних атак?

- **Согласованность мер безопасности:** Насколько уязвима модель к несогласованной реализации мер безопасности и обеспечения соблюдения политики? Насколько велика вероятность того, что цели в сфере безопасности будут достигнуты всеми участниками, отвечающими за работу компонентов системы? Или же на безопасность будут серьезно влиять различия в объеме опыта и инвестиций регистраторов/реестров/проверяющих?

Последствия в плане юрисдикций и конфиденциальности

- **Хранение данных в местных юрисдикциях:** Позволяет ли модель хранить регистрационные данные в одной из нескольких юрисдикций? В какой степени владельцы регистраций или регистраторы/проверяющие могли бы выбрать для хранения регистрационных данных юрисдикцию, где законы о защите данных совместимы с законодательством местной юрисдикции владельца регистрации?
- **Возможность применения местных законов для отображения:** Позволяет ли модель получить доступ к регистрационным данным способом, который совместим с требованиями одной из нескольких юрисдикций? В какой мере СКР могла бы обеспечить применение законов о защите данных, действующих в местной юрисдикции владельца регистрации, к регистрационным данным, доступным через СКР?
- **Возможность соблюдения местных законов о защите данных:** Помогает или препятствует модель соблюдению регистратором и реестром местных законов о защите данных, по действие которых они подпадают? Насколько сложной была бы модель в плане оформления оговорок, необходимых для соблюдения этих законов? Каким образом будет обеспечено соблюдение юридических процедур, необходимых согласно местному законодательству владельца регистрации?

Аккредитация

- **Возможность аккредитации инициаторов запросов:** Позволяет ли модель пользователям, желающим получить доступ к защищенным данным на основе целей, подавать заявки на аккредитацию, получать разрешение и учетные данные для доступа, чтобы затем использовать их для получения надлежащим образом авторизованного доступа к данным? Насколько модель помогает или препятствует полноценному применению такой процедуры для аккредитации инициаторов запросов?

Проверка: Становится ли она проще? Становится ли она дешевле? Делает ли какая-либо система получение защищенных учетных данных удобнее или дешевле?

- **Отслеживание/наказание инициаторов запросов:** Насколько эффективно и надежно модель может регистрировать запросы на доступ к данным и ответы для целей обнаружения злоупотреблений со стороны аккредитованных пользователей (то есть действий, нарушающих условия и положения доступа)? В какой мере модель помогает или препятствует действиям по обеспечению соблюдения обязательств (например, наложению штрафных санкций на пользователей, не соблюдающих требования, чтобы препятствовать будущим злоупотреблениям)?
- **Аудит:** Позволяет ли модель осуществлять аудит запросов на доступ к данным, ответов и сопутствующих операций для оценки результативности процедуры аккредитации и авторизованного доступа к данным?

Функционирование

- **Дружелюбный к пользователю портал:** Позволяет ли модель обеспечить дружелюбное к пользователю представление регистрационных данных при их отображении на веб-портале и возврате в виде соответствующих протоколам ответов на запросы? В какой степени модель поддерживает принципы интернационализации (например, местные наборы символов, перевод ответов на запросы)? Насколько модель способствует единообразному отображению данных всех рДВУ?
- **Отчеты о выборочных аудиторских проверках/проверках точности:** Поддерживает ли модель периодические аудиторские проверки точности и отчеты о точности во всех рДВУ? В какой мере модель способствует эффективному и единообразному обнаружению и обновлению неточных регистрационных данных и повсеместному обеспечению соблюдения политик сохранения точности?
- **Задержка доступа к данным (производительность):** Присуща ли модели неизбежная неэффективность обработки данных, которая способна привести к снижению производительности и не поддается устранению путем увеличения масштаба реализации платформы? Какова относительная величина этой неэффективности (по сравнению с другими моделями) в плане скорости обработки запросов и времени ожидания пользователей, запрашивающих регистрационную информацию?

- **Синхронизация данных:** Требует ли модель синхронизации данных, скопированных из какой-либо системы, с другими системами? Насколько велики эти потребности в синхронизации данных, и насколько проблематичным будет любая временная рассинхронизация (по сравнению с другими моделями)?
- **Доступ владельцев регистрации к собственным данным:** Способствует или препятствует модель доступу владельца регистрации к своим собственным регистрационным данным?
- **Требования к хранению/депонированию:** Вводит ли модель несколько областей хранения, повышающих количество или сложность хранилища данных и требования к депонированию?
- **Возможность предварительной проверки:** Поддерживает ли модель предварительную проверку данных владельца регистрации и целевых контактных лиц во всех рДВУ? В какой мере модель способствует эффективному и единообразному созданию и сопровождению предварительно проверенных контактных данных и повсеместному обеспечению соблюдения всех соответствующих политик сохранения уникальности?

Реализация

- **Сложность инфраструктуры:** Насколько модель менее сложна в целом по сравнению с другими моделями? Например, у более сложной (слабой) модели может быть намного больше систем и интерфейсов, которые потребуют первоначальных инвестиций и постоянного обслуживания.
- **Простота реализации:** Насколько проще будет внедрение данной модели по сравнению с другими моделями? Например, более трудная для реализации (слабая) модель может потребовать изменения большего количества систем.
- **Простота перехода:** Насколько хорошо данная модель способствует плавному переходу от использования сегодняшней WHOIS к использованию СКР нового поколения по сравнению с другими моделями? Здесь более слабой является та модель, которая делает смену существующих процедур более сложной для пользователей, регистраторов и реестров.

Расходы

- **Сокращение затрат реестров и регистраторов на эксплуатацию WHOIS:** Насколько велика вероятность того, что модель снизит текущие затраты регистраторов и реестров на эксплуатацию и обслуживание по сравнению с затратами на нынешнюю систему WHOIS? Здесь более сильной считается та модель, которая сокращает затраты.
- **Более низкая стоимость реализации:** Больших или меньших первоначальных инвестиций потребует модель в целом на новые/измененные инфраструктурные элементы и процедуры по сравнению с другими моделями? Здесь более сильной считается та модель, которая сокращает общую стоимость реализации.
- **Обратные запросы и архивные запросы WhoWas:** Потребует ли модель дополнительных инвестиций для выполнения обратных запросов и архивных запросов WhoWas, отправленных авторизованными инициаторами запросов? В данном случае более сильной считается та модель, в которой общая стоимость оказания таких услуг ниже.

Примеры использования

Сравнение способности этих возможных моделей поддерживать всех пользователей и цели, указанные в первоначальном отчете, в том числе (помимо прочего) следующие примеры использования рДВУ:

- Приобретение доменного имени
- История регистрации доменного имени (включая отслеживание истории регистрации любого доменного имени (WhoWas))
- Доменные имена указанного владельца регистрации (включая обнаружение всех доменных имен, зарегистрированных конкретным владельцем регистрации (обратный запрос СКР))
- Разбирательства в рамках ЕПРД
- Проведение расследования в отношении неправомочного доменного имени
- Ограничение злонамеренной деятельности в Интернете

Анализ стоимости моделей

Чтобы изучить осуществимость моделей ССКР и ИСКР, а также соответствующие затраты, ICANN наняла компанию IBM для выполнения тщательного анализа различий в стоимости этих двух возможных моделей реализации. IBM подготовила итоговый отчет под названием *«Анализ стоимости реализации моделей службы*

каталогов регистрации (СКР)[40]». Выдержка из выводов IBM, заимствованная из отчета этой компании, включена для справки в настоящий документ.

Подход

В течение февраля-марта 2014 года был выполнен анализ бюджетной стоимости и сравнение реализации синхронизированной[41] *и интегрированной реализации СКР. Использовался поэтапный подход:*

- *Этап 1. Сбор основных требований для каждой модели реализации.*
- *Этап 2. Определение и согласование ключевых расчетных параметров и допущений, представленных ICANN и в целом основанных на ежемесячных отчетах о запросах WHOIS, получаемых от реестров рДВУ. Использование указанных допущений для определения ожидаемой рабочей нагрузки системы и разработки базового решения высокого уровня для каждой из этих двух моделей реализации.*
- *Этап 3. Создание модели затрат и выполнение бюджетной калькуляции затрат для каждого базового описания решения.*
- *Этап 4. Формулирование выводов.*

Отправные точки выполнения работ

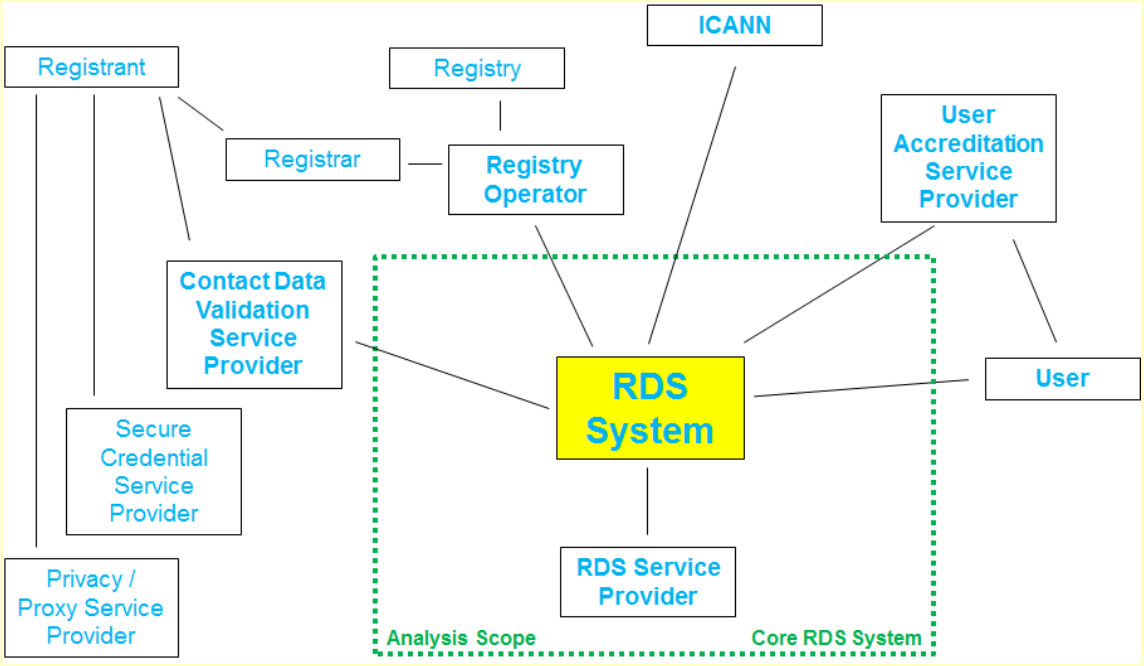
- *Выполнение расчета бюджетной стоимости центральной «системы/ поставщика СКР». Затраты операторов реестров не оцениваются.*
- *Создается модель затрат и смета управляемой услуги. То есть, предполагается создание и постоянное функционирование управляемой услуги СКР и составляется смета соответствующих затрат.*
- *Для целей сравнения стоимости в основу решений и оценки затрат лег главным образом портфель IBM (в первую очередь, предлагаемый IBM продукт SoftLayer IaasS), сторонние компоненты использовались для решения только тогда, когда не существовало альтернатив в портфеле IBM.*
- *Оценка затрат выполнялась только для базового описания требования/ решения, но не для вариантов; никакой детальный анализ факторов, определяющих затраты, не выполнялся.*

[40] https://community.icann.org/display/WG/EWG+Public+Research+Page

[41] Для согласования с итоговым отчетом ЭРГ в настоящем резюме упоминается синхронизированная СКР (ССКР) — модель, которая был описана в предыдущих отчетах ЭРГ как агрегированная СКР (АСКР).

Рамки и расчетные показатели основного анализа

В центре анализа стоимости находилась «Основная часть системы СКР», как изображено ниже



.

Были определены основные поддерживаемые примеры использования для каждой из моделей (синхронизированной и интегрированной).

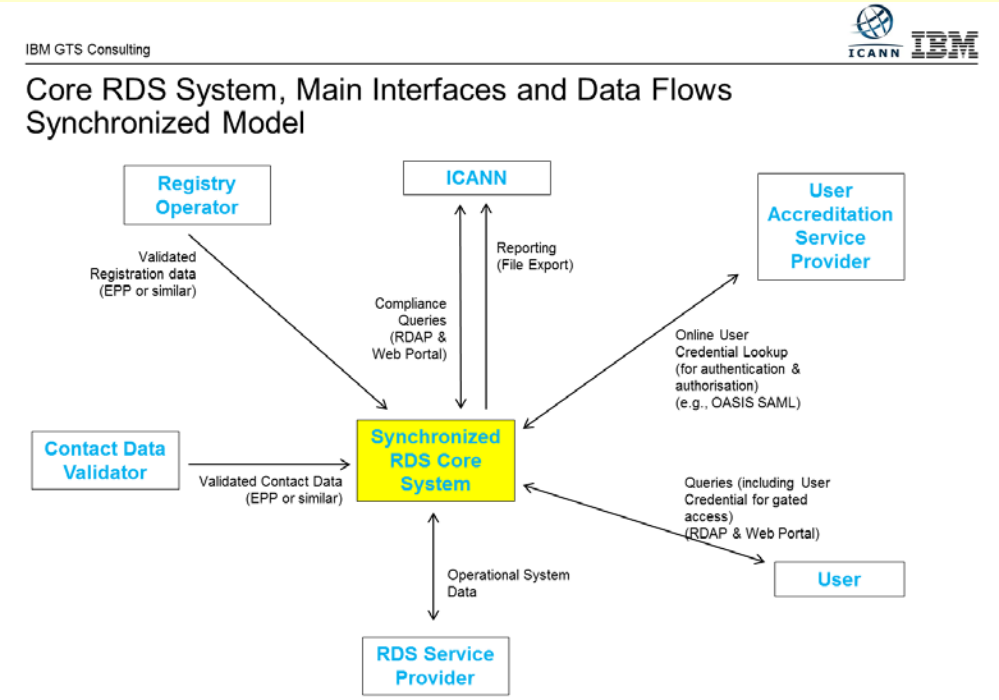
Кроме того, были определены ключевые расчетные показатели и допущения:

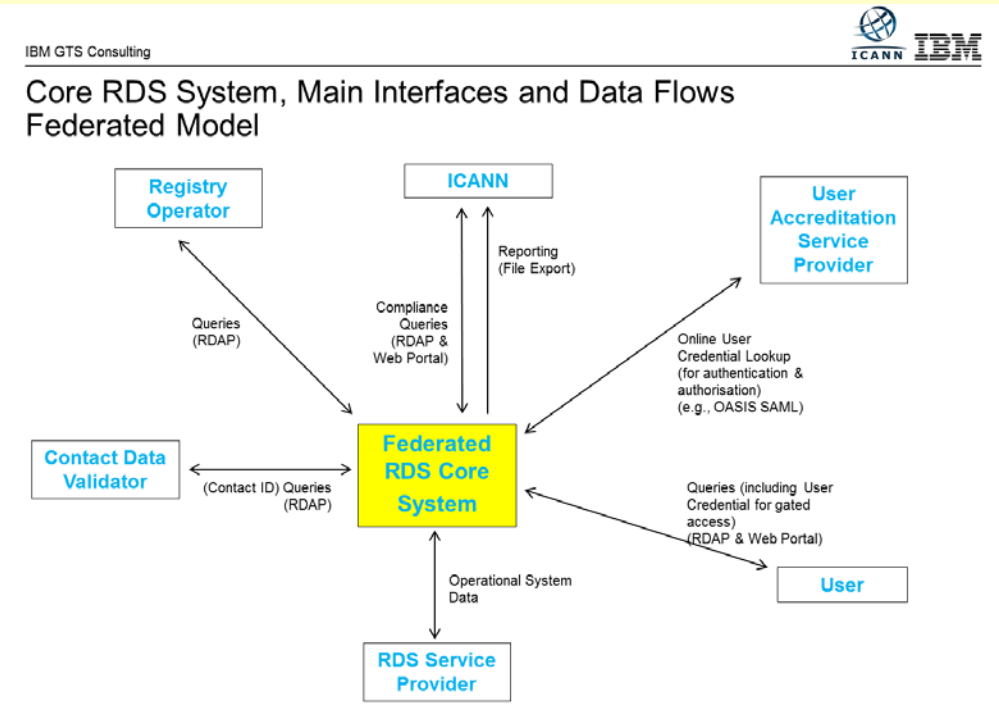
YEARLY GROWTH RATE	22%	nr of DN records added in a year, assumed to include the growth in the nr of gTLDs					
Nr of DN RECORDS, YEARLY UPDATE RATE	100%	nr of DN records updated in a year					
		start yr1 (2015)	start yr2 (2016)	start yr3 (2017)	start yr4 (2018)	start yr5 (2019)	end yr 5 (2020)
	Nr of gTLDs	2000	3000	4000	5000	6000	7000
	growth rate		50%	33%	25%	20%	17%
	December 2013, ICANN input	start yr1 (2015)	start yr2 (2016)	start yr3 (2017)	start yr4 (2018)	start yr5 (2019)	end yr 5 (2020)
NR OF DOMAIN NAMES	151.196.101	184.459.243	225.040.277	274.549.138	334.949.948	408.638.936	498.539.502
NR OF QUERIES/MONTH	9.031.522.529	11.018.457.485	13.442.518.132	16.399.872.121	20.007.843.988	24.409.569.665	29.779.674.992
AVERAGE NR OF QUERIES/SEC	3.484	4.251	5.186	6.327	7.719	9.417	11.489
NR OF QUERIES/PEAK SEC		42.509	51.862	63.271	77.191	94.173	114.891
AVERAGE NR OF QUERIES/HOUR	12.543.781	15.303.413	18.670.164	22.777.600	27.788.672	33.902.180	41.360.660
NR OF QUERIES IN PEAK HOUR	25.087.563	30.606.826	37.340.328	45.555.200	55.577.344	67.804.360	82.721.319
USER VISITS IN PEAK HOUR	16.892.292	20.608.596	25.142.488	30.673.835	37.422.079	45.654.936	55.699.022
CONCURRENT VISITS IN PEAK HOUR	563.076	686.953	838.083	1.022.461	1.247.403	1.521.831	1.856.634
NEW VISITS IN PEAK SEC		28.623	34.920	42.603	51.975	63.410	77.360

% of reverse queries	1,0%

Модели реализации СКР

На основе первоначального отчета и отчета о текущем состоянии дел ЭРГ были получены следующие модели реализации для анализа затрат:



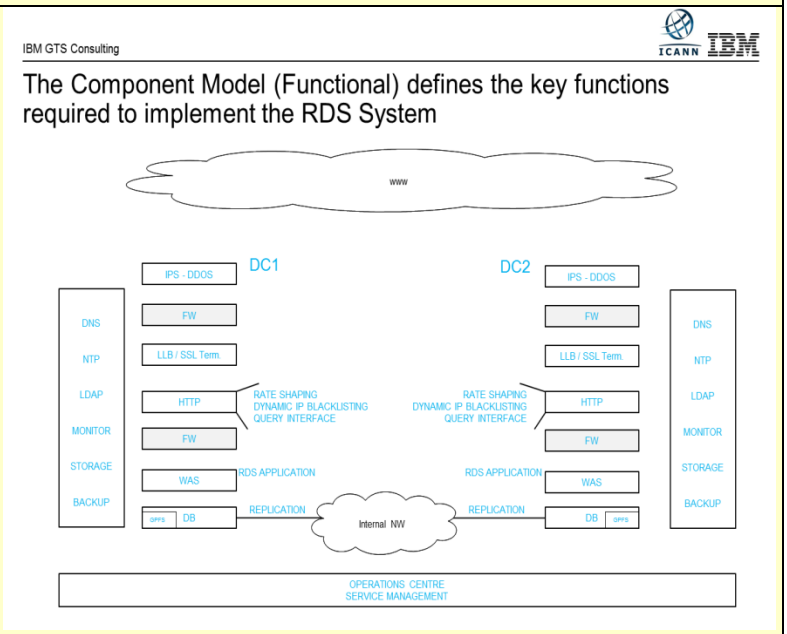


Функциональные компоненты СКР

Для целей анализа стоимости были созданы следующие компоненты модели, содержащие все важнейшие функции, необходимые для реализации системы СКР. При оценке стоимости моделей ССКР и ИСКР использовались допущения, которые соответствуют передовым методам разработки стандартных систем, например реплицирование основной части системы СКР и базы данных в двух географически разнесенных центрах обработки данных с выравниванием нагрузки и переключением при отказе для обеспечения резервирования и доступности, а также IPS для отражения DDoS-атак. Следует понимать, что эти функциональные компоненты ПРИМЕНЯЮТСЯ В ОБЕИХ МОДЕЛЯХ РЕАЛИЗАЦИИ.

Функциональные компоненты:

- *Выравнивание нагрузки/ маршрутизация между ЦОД*
- *Смягчение DDoS-атак через IPS*
- *Выравнивание нагрузки и использование SSL внутри ЦОД*
- *Веб-сервер (HTTP)*
- *Сервер веб-приложений (WAS)*
- *Узел администратора WAS*
- *Система кэширования базы данных (БД)*
- *Система компонентов БД*
- *Сервер хранения*
- *Мониторинг систем*
- *DNS*
- *NTP*
- *LDSP*
- *Хранилище системных журналов*
- *Резервный сервер*
- *Сервер резервного хранения*
- *Клиентская система резервирования БД*
- *Зонирование сети, брандмауэр/IPS*
- *Доступ к Интернету и ЦОД*



Например, структура основной части СКР, содержащая два центра обработки данных, использовалась при оценке как модели ССКР, так и модели ИСКР, при этом применялась архитектура «активный-активный», где каждая основная часть СКР способна обрабатывать до 50% пиковой нагрузки. Анализ стоимости не предусматривал кластеризацию в каждом центре обработки данных для обеспечения высокой доступности; ее можно добавить без изменения относительных затрат на реализацию двух моделей СКР.

Оценки затрат (при предполагаемом количестве обратных запросов 1%)

Приведенная ниже обобщенная оценка затрат ни в каком отношении не является предложением IBM по реализации. Эта оценка была выполнена для одной единственной цели и должна использоваться и рассматриваться только как часть анализа бюджетной стоимости, предназначенного для сравнения двух моделей реализации СКР. На основе ключевых расчетных исходных данных, требований к рабочей нагрузке и приведенного выше описания системного решения, расходы на одно доменное имя в год ***только для основной части систем ИСКР и ССКР*** *оцениваются на следующем уровне:*

Оценка бюджетной стоимости ССКР

€	0,0183	average cost/domain/year

cost per domain name				
yr1	yr2	yr3	yr4	yr5
€ 0,041	€ 0,023	€ 0,017	€ 0,020	€ 0,019

Оценка бюджетной стоимости ИСКР

€	0,0173	average cost/domain/year

cost per domain name				
yr1	yr2	yr3	yr4	yr5
€ 0,041	€ 0,018	€ 0,017	€ 0,021	€ 0,017

Разница в стоимости была дополнительно проанализирована и сравнивается ниже:

FRDS – SRDS Budgetary Cost Estimate Differences

SETUP COSTS		**5,9%**		10,5%	
INFRASTRUCTURE SETUP COSTS	ARCHITECTURE & DESIGN	**1,5%**	0,2%	15,6%	0,0%
	PROVISION & CONFIGURE		1,2%		19,2%
	INFRASTRUCTURE TESTING		0,1%		18,4%
APPLICATION SETUP COSTS	ANALYSIS, DESIGN, CODE, UNIT TEST	**1,2%**	1,2%	0,0%	0,0%
TESTING	INTEGRATION TESTING & DEPLOYMENT	**1,7%**	0,8%	7,8%	0,0%
	E2E SYSTEM TESTING		0,2%		38,2%
	PERFORMANCE		0,2%		33,3%
	SECURITY (ETHICAL HACK)		0,5%		0,0%
TRANSITION TO BAU	TRANSITION TO BAU	**0,6%**	0,5%	26,6%	37,7%
	SERVICE DESK SETUP		0,1%		0,0%
MANAGEMENT	PROJECT MANAGEMENT	**0,9%**	0,9%	13,4%	13,4%

The FRDS model implies a higher computing power requirement (more systems required to handle the envisaged load) in the web and web application server layer.

Due to a higher amount of systems to interface with in an on-line manner when handling queries, the FRDS model is estimated to involve more testing effort

FRDS – SRDS Budgetary Cost Estimate Differences

COST MODEL FRDS		SHARE IN TOTAL		DIFFERENCE WITH ARDS	
		100,0%		-5,4%	
RUN COSTS		**94,1%**		-6,3%	
INFRASTRUCTURE COSTS	PUBLIC NW	**30,5%**	8,1%	-22,4%	-55,9%
	DC NW, GLB, LLB, IPS/DDOS		5,7%		10,7%
	HTTP SERVERS		2,2%		236,0%
	WAS SERVERS		3,7%		218,5%
	DB SERVERS		2,2%		-52,0%
	STORAGE		6,3%		-3,8%
	BACKUP		1,9%		-19,0%
	GENERIC SYSTEMS		0,3%		0,0%
SW LICENCE & MAINTENANCE COSTS	DB	**32,7%**	13,7%	-17,5%	-59,5%
	WAS		18,8%		234,6%
	BACKUP		0,3%		0,0%
OPERATIONS AND MANAGEMENT COSTS	INFRA OPERATIONS & MAINTENANCE	**30,9%**	19,4%	44,0%	63,6%
	APPLICATION OPERATIONS		2,6%		20,0%
	APPLICATION MAINTENANCE		1,3%		27,3%
	SERVICE GOVERNANCE		5,2%		0,0%
	SERVICE DESK		2,4%		100,0%

The Public NW cost is lower in the FRDS case due to the IBM SoftLayer NW charging model: incoming traffic is free; per server 20 TB/month outgoing traffic is free, i.e. you get a total free outgoing volume of #servers x 20 TB per month. As the number of servers increases in the FRDS model, the total amount of free TB outgoing NW volume/month increases.

The FDRS model implies a higher NW throughput requirement. Impact on Firewall and Intrusion Prevention Component.

The FRDS model implies a higher computing power requirement in the web and web application server layer.

The FRDS model implies less storage and backup storage capacity as less data is stored centrally.

The DB compute requirement is estimated to be higher in the SRDS model.

Due to a higher amount of systems to interface with in an on-line manner when handling queries, the FRDS model is estimated to involve a higher application operations, support & maintenance release testing workload

Основные выводы

При использовавшихся допущениях, основная часть СКР немного дешевле при использовании интегрированной модели СКР (ИСКР), чем при использовании синхронизированной модели СКР (ССКР).

Модель ИСКР высокочувствительна к количеству обратных запросов. При более высоком объеме обратных запросов ИСКР становится намного дороже: согласно расчетам, при увеличении нагрузки со стороны обратных запросов с 1% до 3% модель ИСКР становится приблизительно на 35% дороже. Это важный фактор неопределенности и риска, связанный с моделью ИСКР. Предполагается, что модель ССКР, напротив, менее чувствительна к количеству обратных запросов.

Ожидается, что модель ИСКР потребует большего объема усилий по использованию приложений, поддержке, обслуживанию и тестированию, из-за ожидаемого большого объема взаимодействия с реестрами.

Кроме того, модель ИСКР оказывает более существенное влияние на операторов реестров. В модели ИСКР каждому оператору реестра придется реализовать поддержку — в соответствии с соглашением об уровне обслуживания — ответы на запросы в режиме реального времени, в том числе на обратные запросы и запросы архивных данных о владении доменными именами (WhoWas). Для последней категории запросов оператору реестра пришлось бы хранить и обслуживать архивные данные.

ПРИЛОЖЕНИЕ G. ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ ПРОТОКОЛОВ EPP И RDAP ДЛЯ ПОДДЕРЖКИ СКР

Элемент данных	Поддержка EPP для сбора	Поддержка RDAP для доступа
Доменное имя	Да	Да
Состояние регистрации	Да	Да
Серверы DNS	Да	Да
Делегирование DNSSEC	Да	Да
Состояние на стороне клиента	Да	Да
Состояние на стороне сервера	Да	Да
Регистратор	Да	Да
Реселлер	Да	Да
Юрисдикция регистратора	Нет	Нет
Юрисдикция реестра	Нет	Нет
Язык соглашения о регистрации	Нет	Да
Дата создания	Да	Да
Дата первоначальной регистрации	Да	Да
Дата истечения срока действия регистрации	Да	Да
Тип владельца регистрации	Нет	Да*
Имя ЦКЛ	Да	Да
Идентификатор ЦКЛ	Да	Да
Статус подтверждения ЦКЛ	Нет	Нет
Метка времени последнего подтверждения ЦКЛ	Нет	Нет
Организация ЦКЛ	Да	Да
Уличный адрес ЦКЛ	Да	Да
Город ЦКЛ	Да	Да
Регион/штат ЦКЛ	Да	Да
Почтовый индекс ЦКЛ	Да	Да
Страна ЦКЛ	Да	Да
Адрес электронной почты ЦКЛ	Да	Да
Альтернативный адрес электронной почты ЦКЛ	Нет	Да
Телефонный номер ЦКЛ + добавочный номер	Да	Да
Альтернативный телефонный номер ЦКЛ + добавочный номер	Нет	Да
Номер факса ЦКЛ + добавочный номер	Да	Да

Элемент данных	Поддержка EPP для сбора	Поддержка RDAP для доступа
Данные для отправки ЦКЛ SMS	Нет	Да
Данные для отправки ЦКЛ мгновенных сообщений	Нет	Да
ЦКЛ в социальной сети, альтернативная СС	Нет	Да
Контактные данные и URL-адреса ЦКЛ по вопросам злоупотреблений	Нет	Да
Дата обновления	Да	Да
Имя владельца регистрации	Да	Да
Идентификатор контактного лица владельца регистрации	Да	Да
Статус подтверждения контактного лица владельца регистрации	Нет	Нет
Метка времени последнего подтверждения контактного лица владельца регистрации	Нет	Нет
Организация владельца регистрации	Да	Да
Идентификатор компании, являющейся владельцем регистрации	Да	Да
Уличный адрес владельца регистрации	Да	Да
Город владельца регистрации	Да	Да
Регион/штат владельца регистрации	Да	Да
Почтовый индекс владельца регистрации	Да	Да
Страна владельца регистрации	Да	Да
Телефонный номер владельца регистрации + добавочный номер	Да	Да
Номер факса владельца регистрации + добавочный номер	Да	Да
Адрес электронной почты ЦКЛ, альтернативный адрес	Да	Да
Данные для отправки владельцу регистрации SMS	Нет	Да
Данные для отправки владельцу регистрации мгновенных сообщений	Нет	Да

Элемент данных	Поддержка EPP для сбора	Поддержка RDAP для доступа
Владелец регистрации в социальной сети, альтернативная СС	Нет	Да
Контактные данные и URL-адреса владельца регистрации	Нет	Да
URL-адрес регистратора	Нет	Да
Идентификатор IANA регистратора	Нет	Да*
Адрес электронной почты контактного лица регистратора по вопросам злоупотреблений	Нет	Да
Номер телефона контактного лица регистратора по вопросам злоупотреблений	Нет	Да
URL-адрес сайта Internic для отправки жалоб	Нет	Да

*Эти элементы данных не определены в RDAP в явном виде. Они могут быть возвращены при помощи полей «примечания» или расширения протокола.

Расширения и/или дополнения протокола

Юрисдикция регистратора и реестра: Потребуется добавить в EPP или извлекать из текущей информации о местонахождении регистратора. Могут быть возвращены при помощи полей «примечания» субъекта в RDAP или расширения протокола.

Язык соглашения о регистрации: Потребуется добавить в EPP путем расширения протокола.

Тип владельца регистрации: Потребуется добавить в EPP путем расширения протокола.

Статус подтверждения владельца регистрации/ЦКЛ, метка времени последнего подтверждения, альтернативный адрес электронной почты, Альтернативный телефон + доб., SMS, мгновенные сообщения, социальная сеть, альтернативная социальная сеть, URL-адрес для контакта, URL-адрес по вопросам злоупотреблений: Потребуется добавить в EPP путем расширения протокола. RDAP

может обрабатывать идентификаторы социальных сетей, однако потребуется создать спецификацию для определения формата таких идентификаторов.

Тип контактного лица: В настоящее время доступными типами являются «admin» (администратор) «billing» (выставление счетов) и «tech» (технический). Потребуется добавить дополнительные типы контактных лиц в качестве расширений RDAP.

Заявленная цель в запросе RDAP: Потребуется добавить в RDAP путем расширения протокола.

Уровень доступа в EPP: EPP содержит простой механизм сбора и передачи регистратором реестру сведений о предпочтениях владельца регистрации в отношении раскрытия элементов контактных данных, где они могут использоваться для определения поведения системы при ответах по протоколу RDAP. Однако этот механизм недостаточно детализирован для отражения предпочтений на уровне каждого отдельно взятого элемента данных. Поэтому потребуется новое расширение EPP и/или сопоставление контактов для индикации решения владельца регистрации или контактного лица о переопределении используемых по умолчанию параметров раскрытия каждого элемента данных (например, решения опубликовать элемент, который по умолчанию защищен).

Приложение H. МОДЕЛЬ И ПРИНЦИПЫ ПЕРЕДАЧИ И РАСКРЫТИЯ ДАННЫХ

Как отмечалось в разделе VI(b), ЭРГ рекомендует потребовать от аккредитованных служб сохранения конфиденциальности и регистрации через доверенных лиц пересылать всю электронную почту на предназначенный для этого адрес. Цель состоит в том, чтобы предоставить клиентам аккредитованных служб сохранения конфиденциальности/регистрации через доверенных лиц и пользователям СКР, которые могут захотеть связаться с ними, стандартного, всегда доступного и близкого к режиму реального времени коммуникационного канала.

Кроме того, ЭРГ рекомендует потребовать от аккредитованных поставщиков услуг регистрации через доверенных лиц своевременно отвечать на требования о раскрытии сведений (дополнительные подробности приведены ниже). Цель состоит в том, чтобы предоставить пользователям, испытывающим серьезные проблемы из-за доменов, зарегистрированных с помощью услуги регистрации через доверенных лиц, стандартной, всегда доступной и результативной процедуры для поиска эффективного решения проблемы.

При анализе указанных потребностей пользователей ЭРГ заметила еще один недостаток сегодняшней практики работы: отсутствие легкодоступного и эффективного способа поэтапного решения проблемы в случае невозможности установить связь. Многие пользователи быстро переходят к требованию раскрыть сведения, потому что у них нет других средств. ЭРГ рекомендует внедрить процедуру поэтапного решения проблем, которая может оказаться менее затратной для всех сторон и снизит количество проблем, приводящих к более дорогостоящим и требующим большего времени требованиям раскрыть сведения. Этот трехэтапный процесс проиллюстрирован ниже:

Этап 1. Передача

а) Пользователь СКР запрашивает контактные данные для домена, получая при этом:

- Идентификатор контактного лица владельца регистрации (например, идентификатор контактного лица поставщика услуг регистрации через доверенных лиц или клиента службы сохранения конфиденциальности)

- Идентификаторы всех обязательных целевых контактных лиц (ЦКЛ) и опубликованные адреса ЦКЛ (в том числе адреса электронной почты)

- Сообщение о том, что регистрация доменного имени была выполнена через службу сохранения конфиденциальности/доверенных лиц, и

- Имя и адрес аккредитованного поставщика услуг сохранения конфиденциальности или регистрации через доверенных лиц, представленные в виде ЦКЛ поставщика услуг К/Д, которые содержат опубликованные URL-адреса страниц для решения проблем с передачей данных и заполнения формы требования о раскрытии сведений.

б) Пользователь СКР, получая информацию о том, что эта регистрация выполнена через аккредитованного поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц, пытается отправить электронное письмо клиенту этого поставщика по адресу электронной почты для пересылки сообщений. Поставщики могут дополнительно разрешить своим клиентам указывать несколько адресов для пересылки сообщений (например, телефон, номер для SMS, почтовый адрес).

в) Аккредитованного поставщика услуг сохранения конфиденциальности/ регистрации через доверенных лиц необходимо обязать пересылать и получать транслируемые сообщения (например, подтверждения доставки по электронной почте всех сообщений, отправленных на адрес для пересылки). В случае ошибки может быть возвращено сообщение о неполучении (например, «такого почтового ящика не существует»), при этом количество подтверждений для одного отправителя можно ограничить пороговым значением, чтобы препятствовать злоупотреблениям при пересылке.

г) Получивший подтверждение пользователь СКР теперь точно знает, что его сообщение было передано клиенту поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц. Однако этот клиент может принять решение о том, что не будет отправлять ответ, или отвергнуть переданное ему сообщение, не читая (например, посчитав его спамом).

Этап 2. Повышения уровня решения проблемы

Пользователь СКР устает ждать ответа от клиента службы сохранения конфиденциальности/регистрации через доверенных лиц и принимает решение повысить уровень контактов следующим образом:

а) Посещает веб-сайт аккредитованной службы сохранения конфиденциальности или регистрации через доверенных лиц, адрес которого был получен на этапе 1, и заполняет форму для повышения уровня, которая содержит:

- Сведения о личности пользователя СКР (возможно повторное использование учетных данных, которые использовались для запроса к СКР)
- Причина, по которой пользователю СКР необходимо установить контакт (можно использовать раскрывающийся список определенных причин)
- Доменное имя, зарегистрированное через службу сохранения конфиденциальности/регистрации через доверенных лиц
- Загружаемое сообщение, которое необходимо переслать клиенту (возможно зашифрованное?)
- Метку времени первой попытки переслать сообщение

б) Аккредитованного поставщика услуг сохранения конфиденциальности или регистрации через доверенных лиц необходимо обязать предпринять попытку установления прямой связи со своим клиентом, возможно, путем использования контактной информации и/или способов, недоступных пользователю СКР, вернув

этому пользователю «подтверждение доставки» в течение N*[42] дней. Здесь опять-таки, в случае ошибки возвращается сообщение о неполучении (например, «неустановленный пользователь», «истекло время ожидания»), и эти сообщения можно регистрировать и ограничить пороговым значением, чтобы препятствовать злоупотреблениям.

в) Получивший подтверждение пользователь СКР теперь имеет подтвержденное документами доказательство того, что сообщение было доставлено клиенту поставщика услуг сохранения конфиденциальности/ регистрации через доверенных лиц. Этот клиент по-прежнему может не отвечать, но повышение уровня решения проблемы должно способствовать преодолению основных ошибок в канале связи без необходимости направлять требование о раскрытии сведений.

Этап 3. Раскрытие сведений (относится только к доменам, зарегистрированным через доверенных лиц)

Время ожидания пользователем СКР ответа от клиента (владельца лицензии) поставщика услуг регистрации через доверенных лиц истекает, и пользователь принимает решение, что проблема достаточно важна для подачи уголовного или гражданского иска следующим образом:

а) Посещает веб-сайт или совершает телефонный звонок аккредитованному поставщику услуг регистрации через доверенных лиц, идентифицированному на этапе 1, и направляет требование о раскрытии сведений, которое содержит:

- Данные о личности пользователя СКР
- Причина, по которой пользователю СКР необходимо установить контакт (узко ограничена видами ущерба, дающими основания для действия)
- Доменное имя, зарегистрированное через поставщика услуг регистрации через доверенных лиц
- Документацию, подтверждающую нанесение ущерба (данные о регистрации товарного знака, обвинения в злоупотреблении)
- Метку времени попытки переслать сообщение/повысить уровень решения проблемы (номер дела при повышении уровня?)

---

[42] * Время ожидания может зависеть от установленной личности и заявленной причины контакта. Например, 1 день для правоохранительных органов/служб безопасности, расследующих преступление/злоупотребление; 7 дней для владельцев товарных знаков, расследующих нарушение прав на ТЗ; 7 дней для потребителей Интернета, пытающихся связаться с электронными торговцами.

б) Аккредитованного поставщика услуг регистрации через доверенных лиц необходимо обязать расследовать дело и принять надлежащие меры (см. пункт «г»), вернув «ответ на требование раскрыть данные» в течение N*[43] дней. Требования раскрыть данные можно регистрировать и ограничивать видами ущерба, дающими основания для действия, о которых заявляют правомочные пользователи СКР,[44] чтобы препятствовать злоупотреблениям.

в) Аккредитованный поставщик услуг регистрации через доверенных лиц после получения документации, позволяющей рассмотреть дело, может:

- Направить уведомление и передать домен клиенту (то есть, прекратить оказание услуг доверенного лица)
- Временно приостановить работу домена на срок проведения уголовного расследования
- Раскрыть пользователю личность/контактные данные владельца лицензии, занимающегося незаконной деятельностью
- Отклонить требование о раскрытии сведений — подтвердив ответственность доверенного лица за дальнейшее использование домена.

Здесь необходимо разработать политику, подробно определяющую, что следует считать достаточной документацией, и когда следует уведомлять владельца лицензии. Кроме того, нужны четкие политики, определяющие влияние местного законодательства и факторы, которые требуется принимать во внимание. Все описанное выше происходит сегодня в отсутствие какого-либо надзора, руководящих принципов политики или последствий отклонения/игнорирования требований о раскрытии сведений.

---

[43] * Время ожидания может зависеть от инициатора запроса и заявленной причины контакта. Правоохранительные органы могут сразу переходить к этапу 3 (Раскрытие сведений) при проведении оперативных расследований. Временные рамки и усилия на этапе 2 должны быть достаточно малы, чтобы не стимулировать стремление других лиц перейти сразу к этапу 3.

[44] ** Любой пользователь, направляющий требование раскрыть данные, обязан продемонстрировать, что он является стороной, которой нанесен ущерб, дающий основание для действий (или представляет интересы такой стороны). Например, владельцы товарных знаков или их представители, выдвигающие обвинения в нарушении прав на ТЗ, могут продемонстрировать, что они являются владельцами одного или нескольких доменных имен, аналогичных доменному имени, зарегистрированному через доверенных лиц. Необходимо дополнительно обдумать аспекты сопоставления видов пользователей и видов ущерба. В качестве примера см. список вариантов типовых жалоб на домены, зарегистрированные через доверенных лиц, который опубликован на сайте GoDaddy.

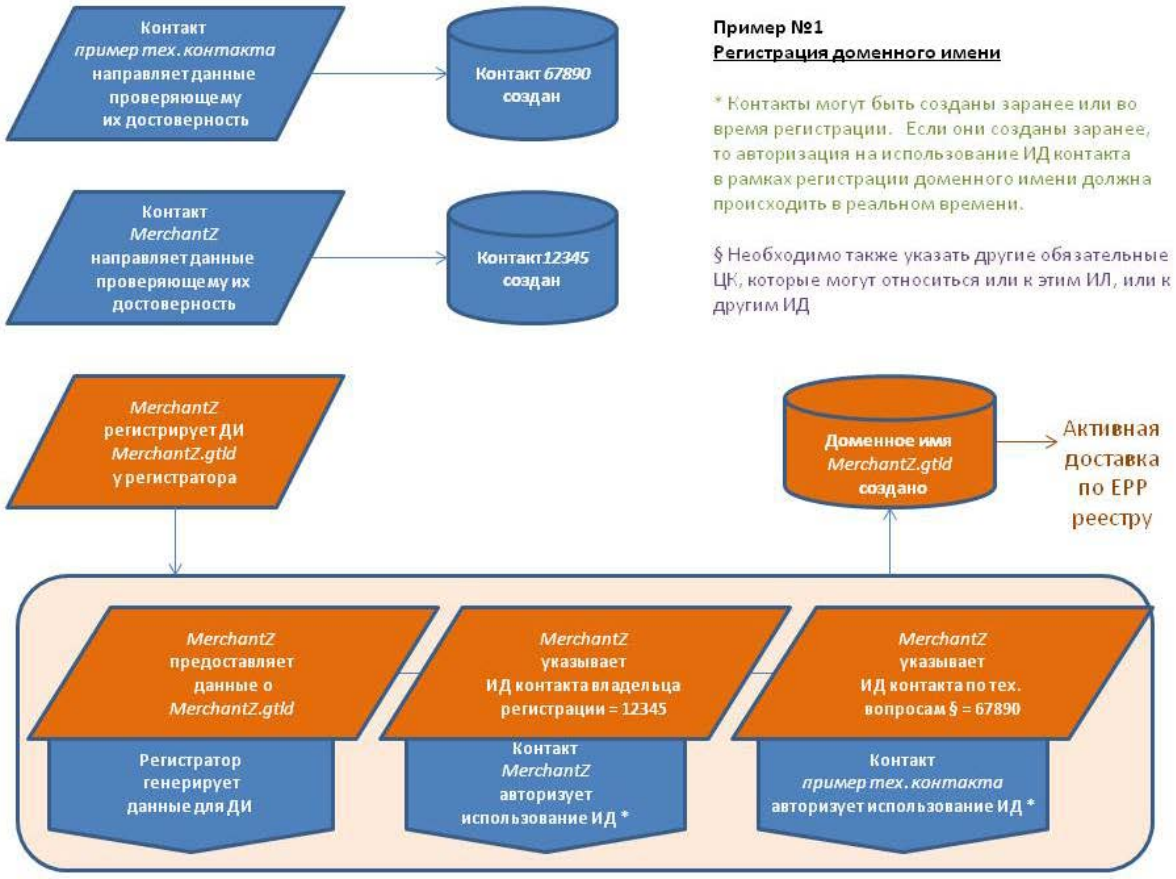
г) Пользователь СКР, получивший ответ на требование раскрыть сведения, теперь располагает информацией, необходимой для прекращения рассмотрения вопроса или для подачи судебного/гражданского иска. Например, нарушение прав на товарный знак может привести в подаче претензии в рамках ЕПРД, в то время как результатом проведенного правоохранительным органом уголовного расследования может стать арест подозреваемого. Если требование раскрыть данные отклонено (или не получен своевременный ответ), пользователь СКР теперь также имеет право подать судебный/гражданский иск против аккредитованного поставщика услуг регистрации через доверенных лиц.

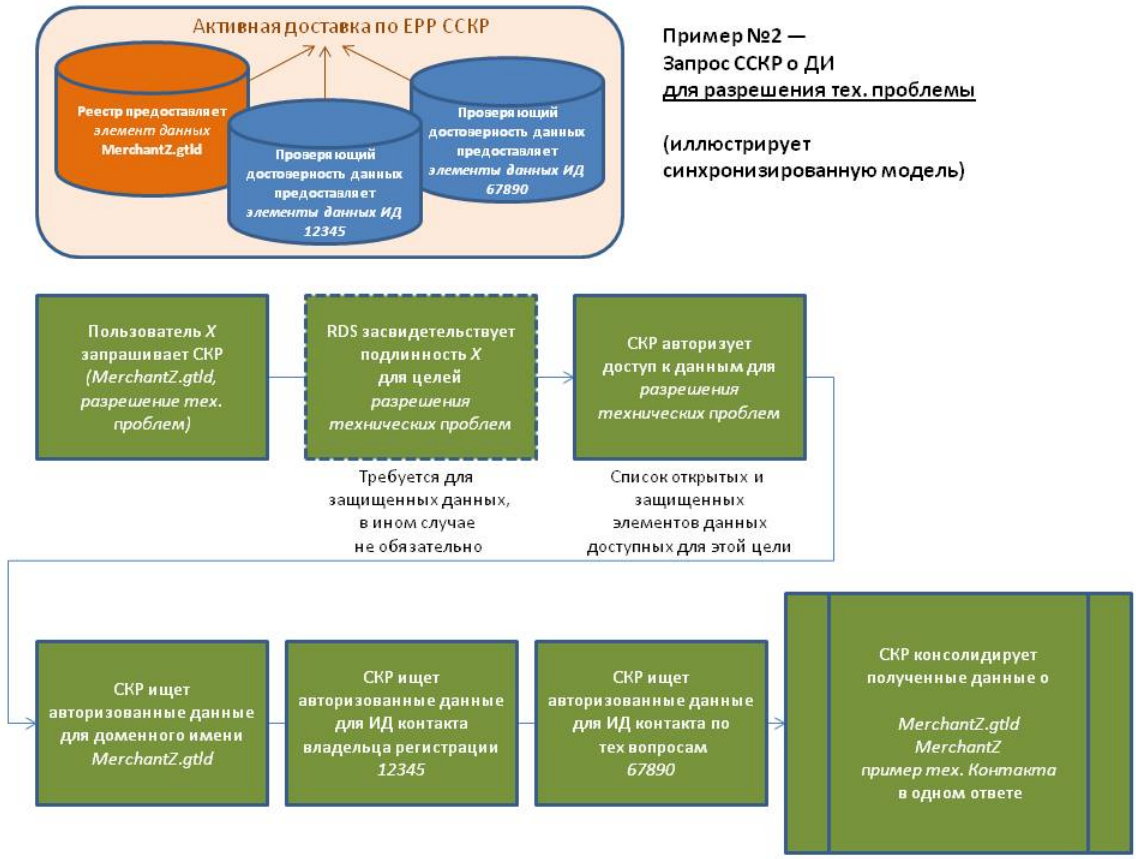
Следует обратить внимание на то, что в описанных выше процедурах не рассматривается, когда необходимо «изобличать публично» владельца регистрации, воспользовавшегося услугами сохранения конфиденциальности или доверенных лиц, вместо того чтобы просто «раскрыть сведения» инициатору требования.

Эти предлагаемые модели и процедуры должны быть дополнительно уточнены РГ ОПРИ PPSAI на основании изучения членами этой группы потребностей сообщества ICANN и получения сведений о передовых практических методах, выявленных в ответах на проведенный ЭРГ интерактивный опрос поставщиков услуг сохранения конфиденциальности и регистрации через доверенных лиц.

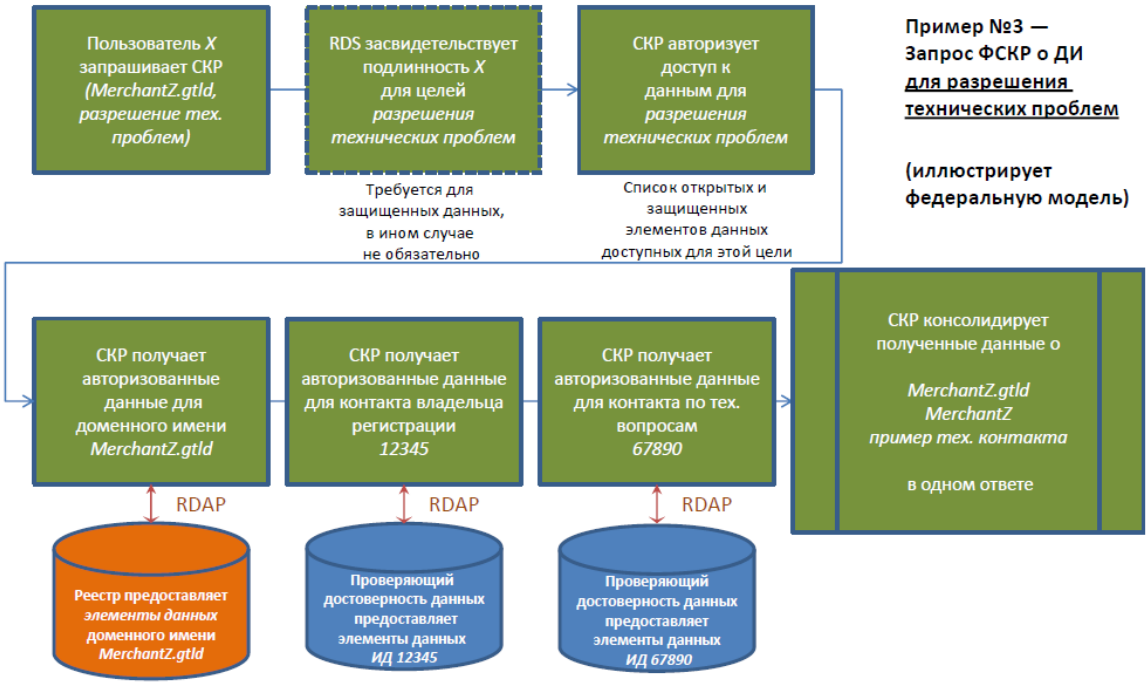
ПРИЛОЖЕНИЕ I. БЛОК-СХЕМЫ ПРОЦЕДУР СКР

Приведенные ниже диаграммы иллюстрируют важнейшие потоки данных между участниками экосистемы СКР во время регистрации доменного имени и запросы лиц, стремящихся получить из СКР информацию о доменном имени для решения технических проблем.





Чтобы содействовать сравнению моделей, тот же самый пример повторно приведен ниже для ИСКР.



ПРИЛОЖЕНИЕ J. ОПИСАНИЕ ЭРГ

Выбор процедуры и концепции

При создании ЭРГ Правление ICANN избрало новаторский подход к решению сложной проблемы, предыдущие попытки решения которой зашли в тупик и стали причиной раздоров. Правление объединило в одну группу людей, представляющих широкий спектр мнений и заинтересованных сторон в надежде, что, обмениваясь опытом друг с другом, они смогут добиться успеха там, где остальные потерпели неудачу. После передачи настоящего итогового отчета и его 180 принципов, получивших единодушную поддержку членов группы, концепция Правления действительно материализовалась.

Члены ЭРГ тщательно отбирались при содействии опытного и объективного посредника, Жана-Франсуа Бариля (Jean-Francois Baril). Он был выбран из-за своего опыта в разработке стандартов для отрасли бытовой электроники. Десятки кандидатов в члены ЭРГ оценивались по нескольким критериям, включая лидерские качества, профессиональные знания, географическое многообразие, навыки достижения согласия, склонность к инновациям и, в некоторых случаях, беспристрастность. Было ощущение того, что не входящие в сообщество ICANN люди способны принести свежий взгляд, не будучи изнуренными предыдущими попытками решить проблему WHOIS.

Состав ЭРГ

В состав ЭРГ входят частные лица, представители Правления и персонала из Австралии, Канады, Китая, Европейской Комиссии, Ирландии, Ямайки, Нигерии, Норвегии, Швейцарии, Великобритании и Соединенных Штатов. Это географическое многообразие способствовало пониманию многих относящихся к работе ЭРГ сложностей, связанных с вопросами юрисдикции.

Среди членов ЭРГ были опытные предприниматели и мировые лидеры — Аджайи (Ajayi), Ала-Пиетиля (Ala-Pietilä), Нейлон (Neylon), Расмуссен (Rasmussen) и Шах (Shah). Их коллективный опыт в уравновешивании рисков и их стиль решения проблем с ориентацией на результат уже на раннем этапе работы проложили дорогу к достижению консенсуса в ЭРГ.

Поскольку в круг обязанностей ЭРГ входило изучение государственной политики, а именно вопросов неприкосновенности частной жизни, опыт работы в государственном секторе был ключом к успеху. Перрин (Perrin) и Нибель (Niebel) поделились своим опытом, накопленным за время работы в государственных органах Канады и Европы, обеспечив выдвижение этих вопросов на передний план при разработке системы следующего поколения. Важно то, что во время своих совещаний ЭРГ была осведомлена и старалась не забывать о последних изменениях в законах Европейского Союза о защите данных.

Другим важным аспектом работы ЭРГ является обеспечение того, чтобы ее рекомендации могли быть реализованы приемлемым образом в сегодняшней экосистеме DNS. Экспертные знания членов группы в области работы регистраторов рДВУ (Нейлон (Neylon)), реестров рДВУ (Холленбек (Hollenbeck) — .com и .net), и нДВУ (.cn — Цзянь (Jian), .uk — Нанайаккара (Nanayakkara), .ng — Аджайи (Ajayi) и .au — Дисспейн (Disspain)) позволили пролить свет на такие вопросы, как подходы к проверке данных, регистрации с сохранением конфиденциальности/через доверенных лиц, совместимость с такими протоколами, как EPP и новый разрабатываемый в IETF протокол RDAP, а также включить такие концепции, как «регулируемый доступ» для отображения конфиденциальных элементов данных.

Вопросы безопасности и стабильности также подверглись изучению благодаря знаниям действующего и бывшего членов ККБС (Крокер (Crocker) и Расмуссен (Rasmussen)), поделившихся своим широким пониманием потребностей правоохранительных органов при противодействии злонамеренному использованию DNS.

Разработка новой системы невозможна без рассмотрения потребностей множества пользователей СКР следующего поколения. В состав ЭРГ входили члены с глубокими знаниями проблем владельцев интеллектуальной собственности (Кавагучи (Kawaguchi), Вейра (Vayra) и Шах (Shah)), которые серьезно опираются на существующую систему WHOIS при борьбе с киберсквоттингом, мошенничеством и контрафактной продукцией в Интернете, а также в группе были участники, поделившиеся пониманием вопросов с точки зрения конечных пользователей (Сэмюэлс (Samuels) и Пфайфер (Phifer)). Многообразие точек зрения помогло обеспечить включение в состав модели законных целей доступа к СКР для получения регистрационных данных и при этом свести к минимуму неэффективность и злоупотребления, которые присущи используемым сегодня процедурам.

Чтобы дополнить состав ЭРГ, в него были включены сотрудники ICANN (Мишель (Michel), Милам (Milam)), которые поделились пониманием вопросов с точки зрения руководства корпорации и знаниями договорной базы ICANN. Консультант (Пфайфер (Phifer)) также предоставила данные о результатах широких исследований WHOIS, проведенных ОПРИ за последние пять лет, чтобы помочь ЭРГ формулировать свои рекомендации на основе фактов.

Рабочая методика

ЭРГ начала свою работу с серии мероприятий, целью которых было знакомство членов группы друг с другом и достижение взаимопонимания, доверия и, что еще более важно, ощущения принадлежности к одной команде. ЭРГ сформулировала совокупность общих ценностей группы для преодоления любых препятствий на пути изучения инновационных решений этой сложной проблемы. Это следующие ценности:

- Работать в группе, сохраняя индивидуальность
- Свобода слова
- Никакой принадлежности к социальным сетям
- Интеллектуальная честность
- Отраслевое саморегулирование
- Свежий подход к проектированию
- Учитывать суровую реальность (технологии и правительства)

Эти ценности помогли направить работу ЭРГ по пути компромиссов, необходимых для разработки СКР и формулирования принципов, которые изложены в настоящем итоговом отчете.

Чтобы получить более подробные сведения и биографии членов ЭРГ, ознакомьтесь с этим объявлением.