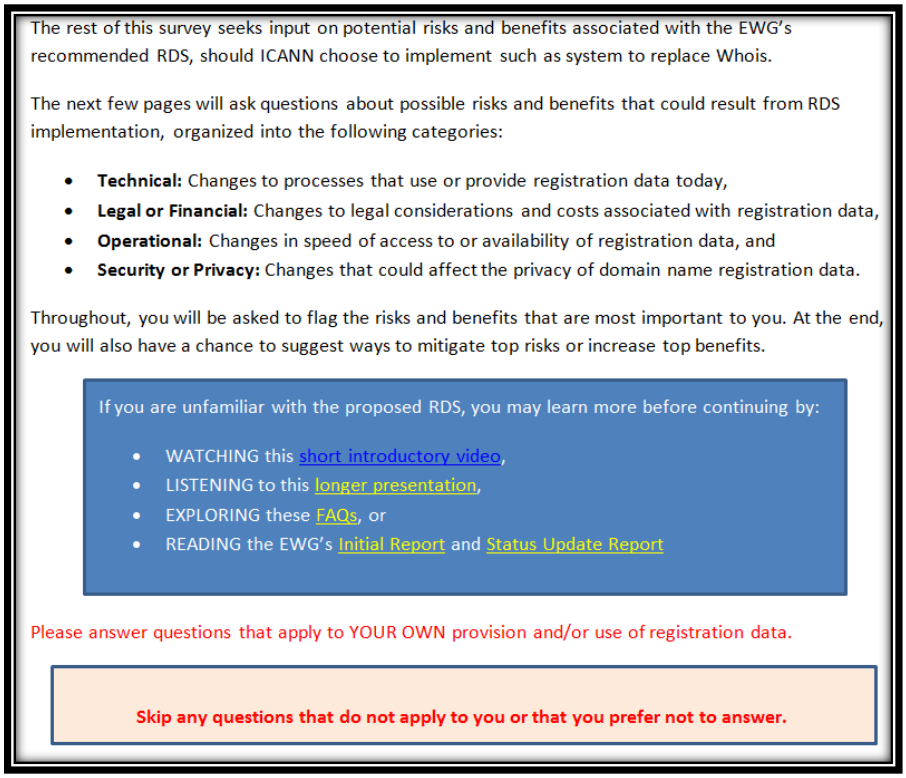
Опрос на тему рисков СКР — сводные результаты

14 марта Экспертная рабочая группа по вопросам справочных служб рДВУ (ЭРГ) предложила всем сторонам, которые предоставляют или используют регистрационные данные доменных имен рДВУ, в том числе пользующимся сегодня данными WHOIS владельцам регистраций, регистраторам, реестрам и широкому спектру физических лиц, компаний и других организаций, принять участие в опросе на тему рисков СКР. Этот опрос позволил респондентам сообщить ЭРГ о рисках и выгодах, которые может им принести **Служба каталогов регистрации следующего поколения (СКР)**.

В настоящем документе сведены воедино все риски и выгоды, которые удалось выявить путем этого опроса. ЭРГ использовала ответы на этот опрос для обнаружения и уменьшения непредвиденных и ненужных рисков при подготовке своего итогового отчета (опубликованного 6 июня 2014 года). ЭРГ также рекомендует использовать эти ответы как исходные данные при выполнении в будущем полной оценки рисков для предлагаемой СКР.

Структура опроса

Показанное ниже введение стало подготовительным разделом для предоставления справочной информации тем, кто не знаком с СКР и систематизацией рисков и выгод по 4 категориям:



The rest of this survey seeks input on potential risks and benefits associated with the EWG's recommended RDS, should ICANN choose to implement such as system to replace Whois.

The next few pages will ask questions about possible risks and benefits that could result from RDS implementation, organized into the following categories:

- **Technical:** Changes to processes that use or provide registration data today,
- **Legal or Financial:** Changes to legal considerations and costs associated with registration data,
- **Operational:** Changes in speed of access to or availability of registration data, and
- **Security or Privacy:** Changes that could affect the privacy of domain name registration data.

Throughout, you will be asked to flag the risks and benefits that are most important to you. At the end, you will also have a chance to suggest ways to mitigate top risks or increase top benefits.

If you are unfamiliar with the proposed RDS, you may learn more before continuing by:

- WATCHING this short introductory video,
- LISTENING to this longer presentation,
- EXPLORING these FAQs, or
- READING the EWG's Initial Report and Status Update Report

Please answer questions that apply to YOUR OWN provision and/or use of registration data.

Skip any questions that do not apply to you or that you prefer not to answer.

Для каждой категории приводились примеры возможных рисков и выгод, и участникам опроса предлагалось сделать следующее:

- *Выберите ВСЕ технические риски, которые могут оказать на ВАС влияние.*
- *Выберите ДВА (2) риска, которые могут оказать на вас наибольшее влияние.*
- *Выберите ДВА (2) наиболее вероятных риска.*
- *Выберите ЛЮБЫЕ новые риски СКР, которые еще не входят в состав известных рисков Whois.*

-- Опубликовано 28 июля 2014 г. --

Опрос на тему рисков СКР — сводные результаты

Участникам опроса также предлагалось добавить другие потенциальные риски и выгоды. В настоящей сводке результатов опроса определены наиболее часто упоминавшиеся риски и выгоды, наряду с вписанными дополнениями.

Обзор ответов

Этот предварительный опрос на тему рисков СКР проводился на английском языке, собрав 182 частичных ответа до 12 июня 2014 года включительно. Немногим более 100 респондентов заполнили анкету опроса целиком.

Все ответы кроме одного были отправлены до опубликования итогового отчета ЭРГ. По существу, эти результаты представляют собой отзывы о СКР в том виде, как она была предложена в отчете о текущем состоянии дел ЭРГ (от 11 ноября 2013 г.) и представлена на 48-й конференции ICANN в Буэнос-Айресе. Эти результаты не следует считать комментариями к окончательным предложениям по СКР, которые подробно сформулированы в июньском отчете ЭРГ 2014 года. Тем не менее, эти ответы помогли ЭРГ понять, что пользователи и поставщики данных Whois считают потенциально важными, значимыми и вероятными рисками и выгодами, связанными с *любой* СКР следующего поколения.

Демография респондентов

- Представленность регионов мира: Северная Америка (68%), Европа (35%), Азия (20%), Латинская Америка (14%), Африка (12%) и Океания (10%)[1]
- Равное количество тех, кто ИСПОЛЬЗУЕТ, и тех, кто ПРЕДОСТАВЛЯЕТ регистрационные данные:
    - 84% используют запросы регистрационных данных из Whois
    - 63% вводят данные и 24% собирают, хранят или пересылают данные Whois
    - К лицам, ИСПОЛЬЗУЮЩИМ данные, относятся владельцы регистраций (45-57%), индивидуальные пользователи Интернета (50%), деловые пользователи Интернета (50%), технический персонал Интернета (40%), исследователи Интернета (41%), дознаватели из служб безопасности (36%), владельцы интеллектуальной собственности (27%), прочие дознаватели (14%), правоохранительные органы (5%) и около 20 других лиц.
    - К лицам, ПРЕДОСТАВЛЯЮЩИМ данные, относятся физические лица (65%), юридические лица (59%), регистраторы (14%), реестры (9%), поставщики услуг регистрации через доверенных лиц (5%) и третьи лица (5%).

Технические риски СКР

- К наиболее часто упоминавшимся (104 ответа) возможным **негативным техническим последствиям** относятся следующие:
    1. У меня больше не будет анонимного открытого доступа ко всем регистрационным данным (69).

[1] Примечание: разрешены множественные ответы; общая сумма превышает 100%

2. Аккредитация для доступа к защищенным данным может оказаться обременительной (65).
3. Возможно, мне придется изменить практику доступа к регистрационным данным (62).

- К наиболее значимым/вероятным рискам были отнесены следующие: 1 и 2 выше.
- Помимо явно перечисленных рисков, были определены дополнительные технические риски:
    - Новая СКР может оказать влияние на лиц, предоставляющие услуги архивных и обратных запросов Whois (8)
    - Может исчезнуть возможность автоматизированного доступа (6)
    - Будет невозможно получить информацию о преступниках, деловых партнерах или кандидатах (3)
    - Может увеличиться задержка при получении данных или регистрации (2)
    - Возможны нарушения прав на неприкосновенность частной жизни (2)
    - Единый источник отказа/технические риски SAC061 (2)
    - Большие информационные массивы для правоохранительных органов и спамеров — двух групп с высокой вероятностью злоупотреблений
    - Исчезнут общедоступные данные с возможностью поиска
    - [Данные для входа], которые я могу использовать, возможно, придется сменить вначале и в процессе работы по причине текучки кадров
    - Перемещение/переход
    - Возникают межюрисдикционные проблемы
    - Полное отсутствие контроля со стороны общественности над регистрационными данными тех регистраторов, которые терпимо относятся к фальшивым данным
    - Для изменения регистрационных данных могут потребоваться сертификаты SSL
    - Нарушает модель делегирования DNS
    - В некоторых обстоятельствах я теряю возможность узнать, кто получает доступ к моим регистрационным данным
    - Я теряю возможность прямого регулирования или ограничения доступа к своим данным
    - Затраты на разработку, контроль качества, проверку и обновление при отсутствии доходов для их компенсации

  Общее примечание: участники опроса указали на то, что это технические риски, хотя многие из них на самом деле относятся к другим видам рисков, учтенным в остальных разделах данного опроса.

Технические выгоды СКР

- К наиболее часто упоминавшимся (89 ответов) возможным **позитивным техническим последствиям** относятся следующие:
    1. Регистрационные данные, к которым я получаю доступ, могут оказаться более точными (58).

2. Доступ к регистрационным данным может стать более единообразным и согласованным (56).
3. Я могу получить лучший доступ к защищенным данным, которые мне действительно необходимы (41).

- К наиболее значимым/вероятным выгодам были отнесены следующие: 1 и 2 выше
- Помимо явно перечисленных выгод, были определены дополнительные технические выгоды:
  - Повышение точности данных (благодаря управлению контактными данными и их подтверждению) (8)
  - Я смогу предоставлять доступ к своим данным только тем лицам, которые имеют на это законное право, вместо опубликования данных для всего мира
  - Мне будет проще находить рецидивистов и серийных киберсквоттеров перед подачей судебного иска или жалобы в рамках ЕПРД, что позволит сберечь деньги и ресурсы моих клиентов
  - Мне всегда придется предоставлять доступ к Whois через порт 43, а это не очень сложно
  - Получаемые регистрационные данные, скорее всего, стали бы более пригодными для применения, полезными и содержательными
  - Передача доменов между регистраторами станет проще (данные WHOIS будут оставаться без изменений, больше не потребуется проводить анализ выходных данных Whois)
  - Уменьшение отрицательных последствий по причине сокращения масштабов массовой переработки данных. Пример: меньше спама

Юридические и финансовые риски СКР

- К наиболее часто упоминавшимся (102 ответа) возможным **негативным юридическим и финансовым последствиям** относятся следующие:
  1. Может сократиться количество свободно доступных для всех регистрационных данных (68).
  2. Могут вырасти мои общие расходы на получение регистрационных данных (66).
  3. Учет доступа к СКР или уведомление может подвергнуть риску активные расследования (51).
- К наиболее значимому/вероятному риску был отнесен следующий: 1 выше
- Помимо явно перечисленных рисков, были определены дополнительные юридические и финансовые риски:
  - Отслеживание нарушителей прав на торговые марки или спамеров может стать более трудной задачей. (3)
  - Время, необходимое для получения доступа к данным, может увеличиться, создавая задержки (3)
  - Отсутствие открытого доступа ко всем данным может ограничить мои возможности внедрения полезных инноваций.

-- Опубликовано 28 июля 2014 г. --

- Слишком большое количество новых ДВУ ведет к повышению расходов и множеству недобросовестных регистраций.
- Отсутствие прозрачности в отношении владельцев веб-сайтов (особенно коммерческих сайтов, где осуществляются денежные операции или ввод личных данных) может создавать риск для потребителей.
- Могут возникнуть трудности в процессе проверки сведений о других доменах, принадлежащих владельцу регистрации, при подтверждении правомочности в домене с ограниченным доступом.
- Отказы не будут локализованы. Одна цель для всех «атак», в том числе юридических, DOS, с целью получения контроля
- Возможно, мне придется указывать несуществующую информацию (например, реальный почтовый адрес, да, есть люди без постоянного места проживания, владеющие зарегистрированными доменами)
- Создание монополии на данные Whois приведет к сдерживанию инноваций и слишком большой централизации власти над «телефонной книгой» Интернета в одном месте.
- В некоторых гипотетических ситуациях мне не хотелось бы делиться частью данных даже с теми людьми, которые в других отношениях могут заслуживать доверия.
- Я хочу, чтобы МОИ данные Whois были доступны для всех заинтересованных сторон, как и сейчас
- Реестры в ЕС и других местах, где действуют законы о защите данных, не смогут экспортировать данные в СКР, что серьезно снизит ее полезность.
- Бремя расходов и возможных юридических последствий возлагается на владельцев регистраций, регистраторов и реестры с минимальными выгодами для этих затрагиваемых сторон и максимальными выгодами для других лиц.

Юридические и финансовые выгоды СКР

- К наиболее часто упоминавшимся (68 ответов) возможным **позитивным юридическим и финансовым последствиям** относятся следующие:
  1. Повышение качества регистрационных данных может привести к уменьшению нерациональности, требующей затрат (42).
  2. Принуждение к соблюдению договорных обязательств, связанных с данными, может стать более полноценным (35).
  3. Возможно, мне будет проще получить законный доступ к защищенным регистрационным данным (35).
- К наиболее значимым/вероятным выгодам были отнесены следующие: 1 и 2 выше
- Помимо явно перечисленных выгод, были определены дополнительные юридические и финансовые выгоды:
  - Мой риск владения обширным объемом личных данных (включая коммерческие данные, относящиеся к частным лицам) существенно снизится.
  - Простота определения связей между владельцами доменов и обнаружения сетей
  - Я мог бы направить ICANN/поставщику СКР обвинения в отсутствии прозрачности и меньшей подотчетности.

-- Опубликовано 28 июля 2014 г. --

Опрос на тему рисков СКР — сводные результаты

Операционные риски СКР

- К наиболее часто упоминавшимся (87 ответов) возможным **негативным операционным последствиям** относятся следующие:
    1. Моему доступу к регистрационным данным может помешать отказ СКР (68).
    2. Мой доступ к регистрационным данным может задержать медленная аккредитация (66).
    3. Мой доступ к регистрационным данным могут замедлить узкие места СКР (65).
    4. Возвращаемые СКР регистрационные данные могут быть не синхронизированы с последними обновлениями (56).
- К наиболее значимым/вероятным рискам были отнесены следующие: 2 и 3 выше
- Помимо явно перечисленных рисков, были определены дополнительные операционные риски:
    - Ответ на запрос на передачу и раскрытие данных от аккредитованных служб сохранения конфиденциальности и регистрации через доверенных лиц может поступать с большей задержкой (7)
    - Наш бизнес может подвергнуться риску вследствие решений по политике СКР.
    - Регулируемый доступ общественности не обеспечивает прозрачность для потребителей в отношении того, кому они платят за услуги, или при вводе личных данных
    - Утечка данных
    - Могут вырасти трудности/задержка при борьбе с сетевым спамом/атаками/проблемами из внешних источников.
    - Защищенные данные для уровня аккредитации могут не соответствовать фактическим требованиям.
    - Произвольные правила будут препятствовать удовлетворению законных потребностей доступа.
    - Я хочу, чтобы ВСЕ стороны получали доступ к МОИМ данным при помощи укоренившихся в настоящее время технологий.
    - Мошеннические сайты, работающие через сетевые партнерские программы, будет проще защитить от правоохранительных органов, поставщиков услуг и обманутых потребителей.
    - Необходимо внедрить и сохранять новый процесс и систему, не нарушая существующего положения вещей.
    - Потеря дополнительного времени, дохода и возможностей из-за возросшего числа первичных контактов с неопытными юристами по вопросам ИС, которые будут совершать злоупотребления или ненадлежащим образом использовать новую систему.

-- Опубликовано 28 июля 2014 г. --

Опрос на тему рисков СКР — сводные результаты

Операционные выгоды СКР

- К наиболее часто упоминавшимся (61 ответ) возможным **позитивным операционным последствиям** относятся следующие:
    1. Ответы на запросы на передачу и раскрытие данных от аккредитованных служб регистрации через доверенных лиц могут поступать быстрее (40).
    2. Возможно, у меня будет более надежный высокоскоростной доступ к регистрационным данным (40).
    3. Доступ к защищенным данным в режиме реального времени с проверкой подлинности может стать быстрее, чем сегодня (39).
    4. Время ответа СКР может стать более единообразным и предсказуемым, чем в Whois (35).
- К наиболее значимым/вероятным выгодам были отнесены следующие: 2 и 4 выше.
- Помимо явно перечисленных выгод, были определены дополнительные операционные выгоды:
    - Агрегированная СКР может обеспечить лучшую поддержку таких функций, как запросы WhoWas и обратные запросы к Whois (7)

Риски СКР для безопасности и конфиденциальности

- К наиболее часто упоминавшимся (70 ответов) возможным **негативным последствиям для безопасности и конфиденциальности** относятся следующие:
    1. Мои регистрационные данные могут стать более уязвимыми к внешним атакам (40).
    2. Мои регистрационные данные могут быть использованы оператором СКР ненадлежащим образом (40).
    3. Возможно, мне потребуется использовать поддающиеся проверке персональные данные для регистрации домена рДВУ (24).
- К наиболее значимым/вероятным рискам были отнесены следующие: 1 и 2 выше
- Помимо явно перечисленных рисков, были определены дополнительные риски для безопасности и конфиденциальности:
    - «Индивидуальные пользователи Интернета» часто являются правообладателями и должны иметь возможность доступа к соответствующей регистрации для расследования нарушений в Интернете (5)
    - Вызывает беспокойство возможность исключения индивидуальных пользователей, которые должны иметь доступ
    - Наличие достоверного телефонного номера или адреса электронной почты крайне важно для расследующих нарушения правообладателей
    - Мои запросы на получение регистрационных данных могут быть использованы оператором СКР ненадлежащим образом

-- Опубликовано 28 июля 2014 г. --

Опрос на тему рисков СКР — сводные результаты

- Возможно, мне придется отказаться от прав, которые у меня есть как у юридического и физического лица одновременно, и выбрать что-то одно, в то время как зарегистрированные и используемые мной доменные имена несомненно поддерживают оба статуса. Таким образом, мне будет предложено отказаться от одной категории прав, хотя юридически я имею право воспользоваться преимуществами обеих категорий.
- Риск для неприкосновенности личной жизни вследствие того, что мои данные как администратора доменного имени станут более доступными
- Утрата возможности регистраций из-за дополнительных требований; у создаваемых компаний может не быть деловых идентификаторов и т. п., но при этом им все-таки будет необходим домен.
- Теперь у внешних злоумышленников есть большая мигающая красная цель.
- Мои личность может быть в принудительном порядке связана с доменом, которым владеет и управляет юридическое лицо, но не я лично
- Имеющие злой умысел частные лица и организации могут использовать возможность скрыть сведения о себе среди защищенных данных, чтобы усложнить для персонала служб безопасности и обеспечения соблюдения обязательств задачу успешного расследования.
- Я не могу зарегистрировать домен анонимно
- Раскрытие причин, по которым мне нужен доступ к данным. Они законны, но это мое дело, не касающееся ICANN.
- Регистрационные данные могут стать менее доступными для служб безопасности, защиты товарных знаков и других органов обеспечения правопорядка из частного сектора.
- Мои регистрационные данные станут более уязвимыми для третьих лиц, в том числе для тех, кто обеспечивает безопасность частной собственности, и для частных фирм, которые захотят получить больший доступ к личной и конфиденциальной информации во многих рДВУ.
- Возможность стать фигурантом судебного процесса в результате связи моего имени с компанией
- Предложение многоуровневого доступа для правоохранительных органов — это способ предоставления им более широкого доступа в обход судебных предписаний и повесток. Это не та возможность или процедура, в которой следует участвовать ICANN.
- Возможность единоличного принятия будущих решений по политике в отношении регистрационных данных.
- Доступ третьих лиц может противоречить местному законодательству, правилам хранения данных или обеспечения конфиденциальности, и без моего ведома может создавать риск судебного преследования для клиентов.
- Доступ третьих лиц или хранение данных может создать инструмент для массового злонамеренного использования данных, принадлежащих мне или моим клиентам.
- Новая система может стать новым направлением для атак.

-- Опубликовано 28 июля 2014 г. --

Опрос на тему рисков СКР — сводные результаты

Выгоды СКР для безопасности и конфиденциальности

- К наиболее часто упоминавшимся (55 ответов) возможным **позитивным последствиям для безопасности и конфиденциальности** относятся следующие:
    1. Мои регистрационные данные могут быть лучше защищены от ненадлежащего использования (37).
    2. Защита моих регистрационных данных может стать более единообразной (31).
    3. Я смогу публиковать идентификатор контактного лица для многократного использования вместо своего имени (29).
    4. Меньшая часть регистрационных данных может стать публичной и доступной анонимным лицам (27).
- К наиболее значимым/вероятным выгодам были отнесены следующие: 2 и 3 выше.
- Помимо явно перечисленных выгод, были определены дополнительные выгоды для безопасности и конфиденциальности:
    - Правила подтверждения, проверки подлинности и авторизации будут применяться последовательно и будут поддаваться аудиторской проверке (7)
    - Я буду сильнее стремиться к обновлению своих контактных данных для сохранения их точности, поскольку у моих преследователей больше не будет к ним доступа
    - Необходимость предоставления юридического, а не физического сертификата
    - Более открытый доступ к юридическим лицам

Дополнительные выводы

Респонденты представили 30 комментариев относительно **неизбежных рисков**, конкретизируя сформулированные ранее риски:

1. Будет ограничен доступ к регистрационным данным, который сейчас является беспрепятственным.
2. Риски 5a, 5b, 9b (изменение практических методов, сокращение открытого публичного доступа) являются неотъемлемой частью СКР.
3. Любая организация, которая контролирует единую центральную точку доступа к регистрационным данным, всегда будет иметь слишком большую власть над общественными интересами.
4. Проблема неограниченного доступа к данным даже лиц, имеющих необходимые полномочия, является вопросом, который сообществу следует изучить глубже. Тот факт, что СКР вряд ли будет проверять чрезмерно широкие операции поиска государственных органов и третьих лиц, создает огромный риск.
5. В случае отказа архитектуры у нас не будет прямого доступа к информации. Или же доступ после аккредитации займет слишком много времени.
6. Возможность получать информацию эффективно и своевременно (для поддержки клиентов, расследующих деятельность мошеннических веб-сайтов)
7. Возможность защиты потребителей от покупок и/или ввода личных данных на мошеннических веб-сайтах (из-за недостаточной прозрачности сведений о владельцах сайтов)
8. Централизованное хранение и предоставление данных Whois для всех регистраций в базе данных любого вида (а не у регистраторов и реестров) повышает вероятность утечки данных.
9. Система, подобная этой, станет магнитом для лиц, занимающихся взломом баз данных, что может привести к многократному замедлению обслуживания и перерывам в работе.
10. Я верю в то, что можно заставить сообщить правильные сведения во время регистрации, но как будет поддерживаться их актуальность?

-- Опубликовано 28 июля 2014 г. --

Опрос на тему рисков СКР — сводные результаты

11. Соблюдение норм ICANN не является единственной причиной предоставления доступа к WHOIS. На практике реестру всегда придется предоставлять доступ к WHOIS и через порт 43, и через порт 80, что увеличит расходы и риск.
12. СКР нарушает фундаментальный принцип Интернета — децентрализацию власти и контроля. Это происходит из-за введения целой совокупности новых межюрисдикционных проблем технически неполноценным образом.
13. Игнорирует следующие проблемы: 1) как мне найти сервер Whois для зоны; 2) «частные» домены, которые открыты для «государственной» регистрации; 3) установленная база, существующие инструменты и практики.
14. Новый механизм предписывает сокрытие многих данных. Это приведет к повышенному риску для общественности, поскольку в отношении [проблемных] доменов не будут приниматься меры и передача по инстанциям. Кроме того, будут потеряны доказательства для правоохранительных органов.
15. Текущая система требует предоставлять большой объем данных. Эти данные уязвимы для перехвата при передаче или в хранилище лицами, имеющими сомнительные нравственные основания, или лицами, имеющими противозаконные намерения.
16. Люди вовлечены — ошибка встроена в систему.
17. Централизация контроля над тем, кто может получить доступ к регистрационным данным доменных имен, и требование выполнить определенную проверку физического или юридического лица, получающего доступ к регистрационным данным доменных имен, создает неизбежный риск монополии и ограничивает возможности правоохранительных органов и следователей из служб безопасности эффективно выявлять злонамеренное поведение в Интернете. Эти риски представляются неизбежными [в любой модели].
18. Неизбежно произойдет замедление процесса регистрации доменов, если теперь будет необходимо проверять регистрационные данные.
19. Предлагается распространить регулируемый доступ к СКР на правоохранительные органы большинства или всех стран. Следовательно, основная цель системы в том, чтобы сделать индивидуальных владельцев регистраций уязвимыми для преследования со стороны иностранных агентств, которым они не обязаны подчиняться и перед которыми не имеют юридических обязательств. Таким образом, СКР по своей природе является дефектной
20. Любой механизм анонимной регистрации будет подвержен злоупотреблениям. Минимальное принуждение злоумышленников регистрироваться с указанием имени и почтового ящика создает небольшое препятствие при получении доступа к регистрационным данным доменов для преступных целей.
21. Открытый доступ и препятствия для массового тиражирования регистрационных данных противоречат интересам спекулятивных операций с регистрациями доменов, поэтому любая новая СКР, созданная ICANN, неизбежно «исправит» эти «проблемы» нынешней Whois.
22. Очевидно, что авторы отчета в качестве основной цели избрали защиту неприкосновенности личной жизни относительно небольшого количества владельцев зарегистрированных доменов, имеющих особые потребности в плане конфиденциальности. Однако законных случаев такого рода чрезвычайно мало... Предлагаемые изменения будут главным образом препятствовать работе «лиц с благими намерениями» и приведут к созданию экосистемы доменов, более подверженной злоупотреблениям и с большей вероятностью наполненной неточными и бесполезными данными.
23. Наличие больших массивов данных, безусловно, создает более высокий риск, которого невозможно полностью избежать.
24. Любая централизация данных создает неизбежный риск единой точки отказа: хакерам, киберпреступникам и субъектам с плохими намерениями, например самопровозглашенным правительствам или правительствам, ущемляющим гражданские права и права человека, придется искать личные данные всего лишь в одном месте.
25. Любое ограничение открытого доступа к информации о личности владельца домена затрудняет борьбу со зловредным программным обеспечением и спамом.
26. Отвратительный послужной список ICANN в плане ведения деятельности и обеспечения соблюдения обязательств сводит к нулю вероятность того, что это будет работать

-- Опубликовано 28 июля 2014 г. --

27. Мои регистрационные данные будут храниться в другой стране, судебной системе которой я не доверяю.
28. Создается впечатление, что новая система СКР серьезно улучшит конфиденциальность регистрационных данных, способствуя в силу этого свободе слова, которую я считаю фундаментом и прекрасным свойством Интернета. Единственное беспокойство в плане неизбежных рисков для меня связано с операторами и сотрудниками, а также людьми и организациями, которые будут или смогут иметь неограниченный и/или нерегулируемый доступ ко всем регистрационным данным.
29. Централизованная служба подвержена рискам, не является необходимой и вовлекает ICANN в решение неприятных правовых проблем, которых можно избежать. Давайте рассмотрим другие возможные решения.
30. Независимо от типа или структуры театра кабуки, который может сопровождать место возникновения СКР или те немногие выгоды, которые эта система могла бы предложить кому-то, кроме правоохранительных органов или владельцев торговых марок, эта СКР будет восприниматься как источник данных для злоупотреблений со стороны государственных органов.

13 респондентов представили подробные ответы и обоснование **приемлемых рисков**:

1. Риск приемлемый, учитывая технические средства устранения неисправностей, которые имеются сегодня (высокопроизводительные вычислительные системы, распределение данных в облаке и отказоустойчивые технологии, повышающие доступность, и т. п. (5)
2. При условии разработки с использованием общепринятых технических решений, предназначенных для обеспечения доступности, должны смягчиться любые проблемы в сфере безопасности.
3. Некоммерческие сайты (где нет функций электронной торговли или требований ввода данных) создают меньший риск для потребителей и защитников прав потребителей (компаний, правоохранительных органов и т. п.). Меньшая прозрачность таких сайтов была бы приемлемой.
4. Возможность соблюдения разнообразных законов о неприкосновенности личной жизни является приемлемым риском, который может оказать влияние на бизнес.
5. Риск нарушения безопасности данных с регулируемым доступом приемлемый, поскольку этот риск все-таки меньше, чем сейчас в условиях открытого доступа к базе данных Whois.
6. Риск использования больших массивов данных можно сделать приемлемым за счет продуманной структуры и оперативного надзора. Недостаточный доступ к необходимой информации для различных уровней регулируемого доступа можно улучшить путем тщательного анализа требований заинтересованных сторон.
7. ICANN стала бы получать меньше «комиссионных сборов» в результате внедрения СКР. Предлагаемая СКР уменьшит объем регистраций, который в настоящее время наблюдается на рынке, из-за своего обременительного характера, когда клиент обязан предоставить большое количество данных, прежде чем сможет совершить первую покупку.

Респондентами были предложены 24 способа **снизить или передать риск**:

1. Принятие мер для повышения точности
2. Рисками отказа/возникновения узких мест в СКР следует управлять путем строгого надзора со стороны оператора СКР.
3. Возможности обратных запросов Whois и запросов WhoWas могут быть встроены в СКР
4. Сокращение количества свободно доступных данных можно компенсировать, если тщательно проанализировать элементы данных, являющиеся сейчас общедоступными, и закрыть публичный доступ только к тем из них, для которых будет выявлена объективная необходимость такой защиты.
5. Разработка необременительной процедуры аккредитации, позволяющей получить учетные данные на длительный срок.
6. Идентификацию использования имени необходимо обосновать. Ответ необходимо давать только на основании претензии. Если запрос имеет силу, можно дать ответ.

-- Опубликовано 28 июля 2014 г. --

7. Получает ли владелец регистрации уведомление о том, что были запрошены данные, и если это так, указана ли в уведомлении запрашивающая сторона?
8. Рисков СКР можно избежать только путем внедрения механизмов проверки в существующую модель. Если желательно, чтобы все регистрационные данные соответствовали конкретному формату, этого можно добиться через политику ICANN, а не через новую СКР.
9. Возможно, какой-то способ разграничения коммерческих и некоммерческих сайтов для повышения прозрачности в отношении коммерческих сайтов позволил бы снизить риск.
10. По крайней мере, часть рисков можно снизить при использовании распределенного подхода, при котором каждый реестр хранит свои собственные данные.
11. Переработать всю схему и собирать минимальное количество контактных данных. Применить стандартные принципы соразмерности, преднамеренной конфиденциальности и конфиденциальности по умолчанию.
12. Потребовать получения ответа от контактных лиц в целесообразные предельные сроки, по истечении которых работу домена можно приостановить в ожидании ответа.
13. Хранить меньше данных.
14. Доступ к Whois может и должен оставаться анонимным и открытым для всех пользователей Интернета.
15. Время обработки при проверке регистрационных данных необходимо сократить в максимально возможной степени, чтобы администраторы доменов могли эффективно и результативно управлять своими доменами с минимальным временем ожидания по причине прохождения процедур проверки.
16. Предоставление потребителям возможности выбора поставщика услуг проверки было бы разумным решением, чтобы эти поставщики стремились к сокращению расходов и времени обработки для сохранения своей конкурентоспособности.
17. Централизация проверки в рамках небольшой группы или обязанность проходить проверку у конкретного поставщика уменьшит стимулы сохранения быстроты и экономической эффективности процедуры.
18. Разрешить полностью анонимную регистрацию доменов любому лицу без предоставления каких-либо регистрационных данных (а не только тем людям, необходимость защиты которых признает некая организация). Если регистрационных данных практически нет, открытый доступ ко всем данным не создает никаких проблем.
19. Запретить анонимную регистрацию.
20. Некоторые риски можно без труда смягчить поэтапным подходом к внедрению СКР, например, сделав любые дополнительные требования к данным необязательными в течение некоторого периода и одновременно обеспечив наличие таких данных в существующей инфраструктуре WHOIS. Это будет означать возможность разработки системы СКР и устранения любых ошибок и проблем без воздействия на существующую систему, а затем, после создания СКР и проработки вопросов интеграции в течение достаточного времени, регистраторы и реестры смогут переключиться на новую систему. В качестве подходящего периода, когда дополнительные данные не являются обязательными, а службы работают параллельно, я предлагаю использовать ~3 года. Это достаточный срок для изменения систем и надлежащего обучения потребителей.
21. Аннулировать все регистрации «через доверенных лиц», принудительно обеспечить точность данных, потребовать от реестров ограничить групповой доступ, ввести обязательный открытый, но ограниченный по скорости доступ ко всем регистрационным данным в Whois и запретить оптовую продажу регистрационных данных реестрами и регистраторами.
22. Устранить финансовые стимулы для регистраторов или других лиц продавать услуги конфиденциальной регистрации. В настоящее время этот бизнес дает устойчивый доход, во многом аналогичный доходу, который телефонные компании получали от номеров, не включавшихся в телефонный справочник. Создать условия, в которых регистраторы *ничего* не получают, предлагая услуги конфиденциальной регистрации или регистрации через доверенных лиц. Ввести комиссионный сбор с владельцев регистраций, которые имеют законную необходимость в сохранении конфиденциальности или регистрации через доверенных лиц, достаточный для демонстрации того, что им действительно требуется такая услуга, с перечислением всех доходов от таких комиссионных сборов общественной благотворительной организации (обеспечивая тем самым отсутствие у ICANN стимула поощрять конфиденциальные регистрации или регистрации через доверенных лиц).

-- Опубликовано 28 июля 2014 г. --

23. Лучшие консультации с целью определения обязательных данных для каждого уровня регулируемого доступа.
24. Чтобы снизить риск злоупотреблений при доступе к конфиденциальным регистрационным данным, право на такой доступ должно подтверждаться юридическими документами, подписанными судьей или другим органом правовой защиты.
25. Чтобы изменить мнение, которое создали Сноуден/Кафка/Оруэлл, о массовых злоупотреблениях в связи с чрезмерным интересом, сделать все операции и запросы доступа к системе на 100% прозрачными для общественности.
26. Чтобы преодолеть сопротивление массовым изменениям, найти способ увеличения пользы и уменьшения непривлекательных сторон для владельцев регистраций, регистраторов и реестров, таких как использование реестрами централизованной системы проверки.

13 респондентов предложили способы достичь **хорошего компромисса между рисками и выгодами**:

1. Потенциальные выгоды зависят от способа реализации (2)
2. Любые риски, связанные с ограничением доступа к (в настоящее время бесплатным и общедоступным) данным, можно уменьшить, если сообщество обеспечит более высокую точность всех данных с регулируемым доступом. Ограничение доступа без повышения точности стало бы крупным изъяном любой предлагаемой новой системы (2).
3. Хотя агрегированная база данных могла бы увеличить риски для безопасности, ситуация поддается улучшению благодаря тщательной разработке, надзору и повсеместно доступной службе, в которой результаты отображаются в единообразном формате, что могло бы сделать эти риски оправданными.
4. Многоуровневый доступ в обмен на улучшение данных (то есть повышение полноты и точности) может стать одним из возможных компромиссов.
5. Предлагаемая СКР дает ряд выгод, которые превышают риски. Удобный доступ к точным данным о владельцах регистраций крайне важен для обеспечения соблюдения прав на интеллектуальную собственность в Интернете. Система СКР, улучшающая доступ и точность этих данных, была бы исключительно полезна для владельцев интеллектуальной собственности и их юристов при устранении нарушений прав на ИС и других сопутствующих злоупотреблений со стороны владельцев регистрации доменных имен и других пользователей Интернета.
6. Если затраты на проверку и сроки проверки можно регулировать и поддерживать на минимальном уровне, преимущества предлагаемой системы могли бы стать взаимовыгодными в плане предлагаемых преимуществ системы. Если затраты не регулировать, издержки значительно превысят выгоды.
7. Повышение качества сведений в базе данных Whois является очень важной задачей и заслуживает усилий. Установление согласованной связи владельцев регистраций со всем их портфелем доменов также является важной задачей и заслуживает усилий, обеспечивая при обнаружении и исправлении неточности в данных контактного лица для одного домена их исправление везде, где эти данные используются.
8. Улучшенный программируемый доступ (без произвольных или непродуманных ограничений скорости и т. п.) также принес бы огромную пользу.
9. Единообразный, надежный и практичный доступ к правильным данным дает безусловную выгоду, поскольку риски можно свести к минимуму благодаря осмотрительной разработке и консультациям.

-- Опубликовано 28 июля 2014 г. --

Опрос на тему рисков СКР — сводные результаты

25 респондентов представили в конце опроса следующие **дополнительные комментарии**.

1. В предложении недостаточно конкретных элементов, существенно улучшающих фактическую точность данных (возможность контакта с владельцами регистраций) относительно уровня, который является базовым для САР 2013 и СИО (в новых рДВУ). Их необходимо сформулировать. Аналогичным образом, более содержательная база данных, предоставляющая расширенные услуги, например архивные данные, могла бы оправдать ограничение открытого доступа к этому ресурсу.
2. Одним из преимуществ для нас является возможность выявления владельцев регистраций, которые пытаются скрыть свою личность для продолжения злонамеренной деятельности и распространения вредоносных программ.
3. Возможность применения пользователями и третьими лицами средств доступа к существующей системе Whois для сохранения данных WHOIS с целью создания архивов является критически важной. Любая предлагаемая система СКР должна обеспечивать такую возможность. Это может происходить либо напрямую через саму СКР, либо косвенно за счет сохранения возможности таких операций с использованием сторонних инструментов/клиентских приложений.
4. Предоставление монопольного контроля над этим общественным ресурсом единственной организации нанесет ущерб всему миру и принесет небольшую пользу, которую можно было бы получить при помощи других, менее централизованных средств.
5. Зачем так много новых рДВУ? Это решение губительно для владельцев брендов, потому что ведет к росту расходов на защиту ИС. Уже сейчас мы наблюдаем множество недобросовестных регистраций, хотя периоды ранней регистрации для большого количества новых рДВУ еще даже не начались. У небольшой компании может оказаться недостаточно средств для регистрации во всех доменах, чтобы избежать недобросовестных регистраций. С другой стороны, расходы на юридические иски высоки.
6. Наличие проверенной Whois представляет крайнюю важность вследствие анонимности Интернета. Мы ищем нарушителей, и неточные данные стали недопустимым явлением.
7. Я полностью поддерживаю усилия по повышению точности данных WHOIS. Это будет позитивным изменением, ЕСЛИ централизованная, закрытая база данных не затруднит получение информации, не замедлит процесс получения информации, не ограничит количество доступно для получения информации, не создаст для компаний длительную процедуру получения аккредитации с целью доступа к информации и не создаст проблемы прозрачности для пользователей сети. Значительная часть моих опасений связана с возможностью сообщества, занимающегося вопросами кибербезопасности, эффективно защищать потребителей от мошеннических веб-сайтов, которые могут получить преимущество благодаря закрытой базе данных.
8. Предлагаемый открытый и регулируемый доступ к определенным элементам данных является хорошим решением. Было бы полезно получить более подробные сведения о приемлемых целях раскрытия данных, об оценке таких кандидатов на получение данных, об ответственности пользователей, получающих доступ к защищенным данным, и т. п., чтобы прокомментировать это.
9. В целом, любое движение в сторону централизации данных существенно повышает риски явного и скрытого взлома, тайной и бесконтрольной слежки со стороны государственных органов, широкомасштабных отказов и политического вмешательства. Хотя некоторые цели создания СКР представляют ценность, они не перевешивают совершенно предсказуемые риски. Самыми значительными для СКР рисками являются перспектива платного доступа к публичным данным WHOIS и/или прекращение открытого доступа к базовой информации для технического управления сетью, включая выделение блоков IP-адресов, физическое местонахождение и почтовые ящики для борьбы со злоупотреблениями. От обсуждения любого предложения, не обеспечивающего защиту публичного доступа и сохранение доступности этих элементов информации, следует отказаться максимально быстро и твердо.
10. Я все еще не понимаю, как мы сможем обеспечить «точность» регистрационных данных. Данные первого дня (при регистрации) — это одна вещь, а «периодические проверки», которые я считаю наиболее важными, — другая. По-моему, мы могли бы поручить выполнение проверки «агентствам» на местах (в каждой стране или, может быть, городе), однако при этом снова могут возникнуть некоторые вопросы относительно точности и стандартов.

-- Опубликовано 28 июля 2014 г. --

Опрос на тему рисков СКР — сводные результаты

11. Двумя группами лиц, которым обычный реестр не хотел бы предоставлять массовый доступ к данным Whois, являются спамеры и правоохранительные органы. Предоставление больших объемов информации любой из этих групп нанесло бы непоправимый ущерб репутации реестра. Централизованная система СКР предлагает реестру передать свою репутацию в руки третьего лица.
12. Необходимо признать, что не все стороны пользуются одинаковым протекционизмом в рамках местного законодательства, что международные требования могут остаться невыполненными из-за внешнеполитических проблем. После внедрения СКР будет утрачен крайне важный для борьбы с организованной киберпреступностью ресурс.
13. Как индивидуальный владелец регистрации, в настоящее время я использую функцию сохранения конфиденциальности/регистрации через доверенных лиц своего регистратора, чтобы защитить сведения о своей личности от случайного, ненужного доступа широкой общественности. Я считаю эту функцию необходимой мерой предосторожности, которая предотвращает анонимное личное давление. Мне хотелось бы увидеть такие функции защиты конфиденциальности в составе обязательных и постоянно доступных услуг любого регистратора, чтобы обеспечить создание полностью конкурентного рынка для всех регистраторов, а не только для их произвольно выбранного подмножества.
14. Наибольшую озабоченность у меня вызывает риск, связанный со стоимостью подтверждения моих регистрационных данных и проверкой подлинности в процессе моего доступа к защищенным данным. У меня также вызывают озабоченность сроки обработки и общее замедление по причине введения этих процедур.
15. СКР — прекрасная идея. Если ее правильно воплотить в жизнь, это поможет решить многие проблемы. С нетерпением жду предложений. Однако этот конкретный опрос имеет плохую структуру.
16. Честно говоря, эта система по-видимому является такой же непродуманной, как и доступные в настоящее время услуги «сохранения конфиденциальности WHOIS». Их использование просто наносит ущерб прозрачности организации и, следовательно, ее репутации в Интернете. Спасибо за то, что выслушали меня.
17. Я не вижу никаких выгод, но вижу множество рисков ненадлежащего использования или воровства данных. В идеальном случае можно было бы избежать необходимости предоставления регистрационных данных регистратору. В отсутствие регистрационных данных нет риска злоупотреблений или воровства.
18. У меня вызывает озабоченность возможность справиться с различными видами сетевых атак, спамом, вторжениями, слишком интенсивными потоками данных и т. д. АБСОЛЮТНО необходимо наличие реального контактного лица и гарантии того, что это контактное лицо действительно займется решением тех сетевых проблем, о которых будет проинформировано. Это означает, что контактное лицо должно иметь и полномочия, и техническую возможность обеспечить, чтобы его домен не был источником злоупотреблений. В нынешней системе, особенно для тех доменов, которые скрыты за поставщиками услуг регистрации через доверенных лиц, НЕТ гарантии того, что регистратор/доверенное лицо будет (или сможет) своевременно решать эти вопросы. Если будет разрешено использовать доверенных лиц, необходимо АБСОЛЮТНО четко обеспечить, чтобы любые лица, указанные в ответе на поисковые запросы общедоступных данных, несли ответственность за поведение домена, который они защищают, включая полноценную возможность отключения домена в случае серьезных сетевых злоупотреблений.
19. Самым большой риск создает способ управления доступом к «защищенной» информации, например, будет ли это связано с уплатой комиссионных сборов и насколько обременительной окажется процедура аккредитации для получения доступа. Если это будет сопряжено с большими расходами или будет обременительно, то это серьезно помешает основным деловым операциям, установлению связи с владельцами доменов, исследованиям и многочисленным другим областям управления доменами и изучения доменов.
20. Я считаю этот предлагаемый процесс решением, которое нацелено на создание проблемы и основано на лицемерных липовых аргументах людей, руководствующихся категоричными политическими взглядами.

-- Опубликовано 28 июля 2014 г. --

21. Я не верю, что было уделено тщательное внимание сравнительному анализу требований к конфиденциальности физических и корпоративных/коммерческих юридических лиц. Индивидуальные владельцы регистраций/физические лица должны быть доступны для контакта тем или иным образом, чтобы существовала возможность устранения проблем, оказывающих влияние на других, однако они во всех случаях должны иметь право на сохранение анонимности, кроме случаев получения соответствующего юридического требования. В противоположность этому, юридические лица, за очень немногими исключениями (такими как организации по защите женщин, некоторые подвергающиеся риску политические организации) НЕ ДОЛЖНЫ иметь право на анонимность. Абсолютно неприемлемо, особенно в случае коммерческих предприятий, чтобы они функционировали анонимно, и к их данным НЕОБХОДИМО предоставить открытый и анонимный доступ. Во-вторых, должна существовать процедура, которая позволяет устранить анонимность организаций, не продемонстрировавших свое соответствие критериям сохранения анонимности.
22. Нам причиняют множество неприятностей спамеры и ботсети, использующие фальшивые данные, чтобы скрыть факт владения доменным именем. Данные Whois могут и должны быть понятными и четко определенными. Получение услуг хостинга у других организаций не требует чрезмерных усилий, однако ясность в вопросе о том, кто отвечает за серверы DNS конкретного домена, полезна в операционном плане.
23. По-моему, конфиденциальность намного важнее открытого доступа к регистрационным данным.
24. Поскольку это не приносит никакой пользы, прекратите заниматься тем, что вы делаете сейчас. Если что-то работает, это не нужно ремонтировать. Не забывайте о том, что ряд владельцев регистраций ДЕЙСТВИТЕЛЬНО ЖЕЛАЕТ сохранить доступ к своим регистрационным данным Whois в том виде, как он предоставляется сейчас, а те, кто этого не желает, могут беспрепятственно воспользоваться почтовым ящиком или услугами защиты конфиденциальности, которые предлагают регистраторы.
25. СКР представляет собой слишком большое единовременное изменение и является плохой идеей. Она возлагает бремя на тех, кто получит наименьшую выгоду, не создавая реальных затрат для тех, кто получит наибольшую выгоду.

И наконец, приблизительно 5 из 182 респондентов заполнили большинство полей для произвольного текста язвительными ответами, которые не имели прямого отношения к заданным вопросам, а вместо этого содержали заявления о том, что СКР — плохая идея, которая не принесет никакой пользы.

-- Опубликовано 28 июля 2014 г. --