ICANN | GNSO

Организация поддержки родовых имен

Итоговый отчет по фазе 2 ускоренного процесса формирования политики в области Временной спецификации для регистрационных данных в gTLD

31 июля 2020 года

Статус этого документа

Это итоговый отчет с рекомендациями Группы по ускоренному процессу формирования политики GNSO (EPDP) в области Временной спецификации для регистрационных данных в gTLD, подготовленный в рамках фазы 2 для передачи Совету GNSO.

Преамбула

Целью этого итогового отчета является документирование следующих аспектов деятельности Группы по EPDP: (i) результаты обсуждения вопросов устава группы, (ii) полученные комментарии относительно первоначального отчета по фазе 2 EPDP и их последующий анализ Группой по EPDP, (iii) рекомендации по политике с указанием соответствующих уровней консенсуса и (iv) указания по реализации, представленные на рассмотрение Совета GNSO.

Содержание

Настоящий документ был переведен на несколько языков только для информационных целей. Оригинал и аутентичный текст документа (на английском языке) находится по адресу: https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf

1 Основные положения

1.1 Справочная информация

17 мая 2018 года Правление Интернет-корпорации по присвоению имен и номеров (ICANN) утвердило Временную спецификацию для регистрационных данных в gTLD («Временная спецификация»). Временная спецификация вносит изменения в требования действующих Соглашений об аккредитации регистраторов и Соглашений об администрировании доменов верхнего уровня, чтобы обеспечить соответствие Общему регламенту по защите данных (GDPR) Европейского союза.[1] В соответствии с Уставом ICANN, срок действия Временной спецификации истекает 25 мая 2019 года.

19 июля 2018 года Совет GNSO инициировал Ускоренный процесс формирования политики (EPDP) и учредил Группу по EPDP в области Временной спецификации для регистрационных данных в gTLD. В соответствии с уставом, количество участников Группы по EPDP было прямо ограничено. Тем не менее, в группу по EPDP вошли представители от всех групп заинтересованных сторон, групп интересов и организаций поддержки ICANN, заинтересованных в участии.

В ходе фазы 1 Группе по EPDP было поручено определить, должна ли Временная спецификация для регистрационных данных в gTLD стать частью согласованной политики ICANN в своем нынешнем виде или с изменениями. Этот итоговый отчет касается вопросов фазы 2 устава Группы по EPDP, к которым относятся: (i) обсуждение системы стандартизованного доступа к закрытым регистрационным данным и их раскрытия, (ii) вопросы, отмеченные в Приложении к Временной спецификации для регистрационных данных в gTLD («Важные вопросы, подлежащие дальнейшему рассмотрению сообществом») и (iii) неразрешенные вопросы, отложенные по результатам фазы 1, например вопрос юридических и физических лиц, вымарывание поля «город» и т. д. Дополнительная информация приведена здесь.

Для организации своей деятельности Группа по EPDP договорилась разбить темы, над которыми она работает, на два уровня приоритетности. Приоритет 1 охватывает SSAD и все непосредственно связанные с этим вопросы. Приоритет 2 включает следующие темы:

[1] Текст GDPR приведен по адресу https://eur-lex.europa.eu/eli/reg/2016/679/oj; для получения информации по GDPR см. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/.

- Отображение информации аффилированных и аккредитованных провайдеров услуг сохранения конфиденциальности/регистрации через доверенных лиц
- Юридические и физические лица
- Вымарывание поля «город»
- Срок хранения данных
- Потенциальная цель для офиса технического директора ICANN
- Осуществимость использования единого обезличенного адреса электронной почты для уникальных контактных лиц
- Точность и система учета достоверности данных WHOIS

Группа по EPDP согласилась, что в первую очередь необходимо завершить обсуждение вопросов с приоритетом 1. Однако было решено, что там, где это возможно, группа также будет стремиться параллельно работать над вопросами с приоритетом 2.

1.2 Первоначальный отчет и дополнение к первоначальному отчету

7 ноября 2020 года Группа по EPDP опубликовала свой первоначальный отчет для общественного обсуждения. В первоначальном отчете были изложены основные вопросы, обсуждаемые в связи с предлагаемой Системой обеспечения стандартизованного доступа к закрытым регистрационным данным gTLD и их раскрытия (SSAD), а также предварительные рекомендации.

26 марта 2020 года Группа по EPDP опубликовала дополнение к первоначальному отчету для общественного обсуждения. Дополнение касается предварительных рекомендаций и выводов Группы по EPDP по указанным выше вопросам с приоритетом 2.

После публикации первоначального отчета и дополнения к нему Группа по EPDP: (i) продолжила процесс запроса рекомендаций по правовым вопросам, (ii) внимательно ознакомилась с комментариями общественности, поступившими в ответ на опубликование первоначального отчета и дополнения к нему, (iii) продолжила анализ незавершенной работы вместе с группами сообщества, представители которых являются членами Группы и (iv) продолжила обсуждение подготовки итогового отчета, который будет рассмотрен Советом GNSO и, в случае утверждения, передан Правлению ICANN для принятия в качестве согласованной политики ICANN. В соответствии с требованиями Руководства для Рабочих групп GNSO председатель Группы по EPDP провел опрос, чтобы оценить уровень консенсуса по каждой рекомендации, включенной в состав итогового отчета, как описано в Приложении D. Вкратце:

- 11 (одиннадцать) рекомендаций получили статус «полный консенсус» (№ 1, 2, 3, 4, 11, 13, 15, 16, 17, 19 и 21).
- 3 (три) рекомендации получили статус «консенсус» (№ 7, 20 и 21).
- 6 (шесть) рекомендаций получили статус «значительная поддержка при наличии существенной оппозиции» (№ 5, 8, 9, 10, 12 и 18).
- 2 (две) рекомендации получили статус «расхождение во мнениях» (№ 6 и 14).

Дополнительные сведения об этих статусах см. в Приложении D, а также в разделе 3.6. Руководства для Рабочих групп GNSO.

Рекомендации для рассмотрения Советом GNSO (полный текст рекомендаций см. в главе 3):

Рекомендации по SSAD:

Recommendation #1. **Аккредитация**

Recommendation #2. **Аккредитация правительственных организаций**

Recommendation #3. **Критерии и содержание запросов**

Recommendation #4. **Подтверждение получения**

Recommendation #5. **Требования к ответам**

Recommendation #6. **Уровни приоритета**

Recommendation #7. **Цели подателя запроса**

Recommendation #8. **Авторизация сторон, связанных договорными обязательствами**

Recommendation #9. **Автоматизация обработки запросов в SSAD**

Recommendation #10. **Определение Изменяемых SLA для сроков ответа в SSAD**

Recommendation #11. **Условия и положения SSAD**

Recommendation #12. **Требование к раскрытию данных**

Recommendation #13. **Политика запросов**

Recommendation #14. **Финансовая устойчивость**

Recommendation #15. **Ведение журналов**

Recommendation #16. **Аудиторские проверки**

Recommendation #17. **Требования к отчетности**

Recommendation #18. **Анализ реализации рекомендаций по политике в отношении SSAD с помощью Постоянного комитета GNSO**

Рекомендации с приоритетом 2:

Recommendation #19. **Отображение информации аффилированных и аккредитованных провайдеров услуг сохранения конфиденциальности/регистрации через доверенных лиц**

Recommendation #20. **Поле «город»**

Recommendation #21. **Хранение данных**

Recommendation #22. **Цель № 2**

Выводы по вопросам с приоритетом 2:

Вывод 1. **Цель OCTO**

Вывод 2. **Точность и система учета достоверности данных WHOIS**

Ввиду внешних взаимозависимых элементов и ограничений по времени в этот итоговый отчет входят не все вопросы с приоритетом 2. В частности, не рассматриваются следующие вопросы:

Юридические и физические лица: Хотя этот вопрос на самом деле рассматривался в рамках фазы 2, это не привело к согласованию новых рекомендаций по политике. Материалы запрошенного исследования по этой теме были получены слишком поздно, чтобы должным образом их рассмотреть. В связи с этим и согласно рекомендациям фазы 1 EPDP, регистраторам и операторам регистратур разрешено, но не вменяется в обязанность проводить различия между владельцами доменов в зависимости от того, являются ли они физическим или юридическими лицами. Дальнейшая работа по этому вопросу (включая рассмотрение результатов проведенного корпорацией ICANN исследования под названием «Разграничение юридических и физических лиц в службе каталогов регистрационных данных доменных имен (RDDS)») находится на рассмотрении Совета GNSO.

Возможность наличия у уникальных контактных лиц единого обезличенного адреса электронной почты: Группа по EPDP получила правовые рекомендации, в которых говорится, что публикация адресов электронной почты с одинаковыми масками приводит к публикации персональных данных; это говорит о том, что широкое опубликование маскируемых адресов электронной почты в настоящее время не представляется возможным в рамках GDPR. Дальнейшая работа по этому вопросу рассматривается Советом GNSO.

Группа по EPDP проконсультируется с Советом GNSO о том, как решить оставшиеся вопросы с приоритетом 2.

1.3 Выводы и дальнейшие действия

Настоящий итоговый отчет будет передан Совету GNSO для рассмотрения и утверждения.

1.4 Другие важные разделы этого отчета

Для полного обзора проблем и соответствующих действий Группы по EPDP в итоговый отчет включены следующие разделы:

- Общие сведения о рассматриваемых вопросах.
- Перечень участников обсуждений в Группе по EPDP, в том числе ведомости посещаемости и ссылки на заявления о заинтересованности, где это возможно.
- Приложение, в котором приведен мандат Группы по EPDP согласно ее уставу, принятому Советом GNSO.
- Документация по запросам комментариев сообщества через официальные каналы SO/AC и SG/C, в том числе ответы.

2 Подход Группы по EPDP

В этом разделе представлен обзор методологии работы и подхода Группы по EPDP. Описанные ниже моменты нацелены на то, чтобы читатель получил значимую справочную информацию о дискуссиях и процессах в Группе по EPDP, и не должна рассматриваться как полная информация о работе и дискуссиях в Группе по EPDP.

2.1 Методология работы

2 мая 2019 года Группа по EPDP начала обсуждение вопросов фазы 2. Группа по EPDP решила продолжить работу преимущественно в формате телеконференций, которые проводятся один или несколько раз в неделю, в дополнение к обмену мнениями по электронной почте через лист рассылки. Кроме того, Группа по EPDP провела четыре очных совещания: первая серия личных встреч состоялась на открытой конференции ICANN65 в Марракеше, два специальных очных совещания — второе и четвертое — прошли в штаб-квартире ICANN в Лос-Анджелесе в сентябре 2019 года и январе 2020 года, а третье очное обсуждение состоялось на открытой конференции ICANN66 в Монреале. Материалы всех совещаний Группы по EPDP размещены в ее рабочем вики-пространстве, включая лист рассылки, проекты документов, справочные материалы и комментарии, поступившие от организаций поддержки и консультативных комитетов ICANN, в том числе от групп заинтересованных сторон и групп интересов GNSO.

Группа по EPDP также подготовила план работ, который регулярно пересматривался и обновлялся. Для облегчения работы Группа по EPDP использовала шаблон, чтобы свести в таблицу все данные, полученные в ответ на ее запрос о заявлениях групп интересов и групп заинтересованных сторон (см. Приложение D). Этот шаблон также использовался для записи информации, поступающей от других организаций поддержки и консультативных комитетов ICANN, и его можно найти в Приложении D.

Группа по EPDP провела на открытой конференции ICANN66 в Монреале заседание сообщества, в ходе которого представила всему сообществу ICANN свою методологию и предварительные выводы в целях обсуждения и получения обратной связи.

2.2 Интеллект-карта, рабочие таблицы и структурные элементы

Чтобы обеспечить общее понимание тем, подлежащих рассмотрению на фазе 2, Группа по EPDP отобразила эти темы на следующих интеллект-картах,

что позволило перегруппировать и объединить темы (см. интеллект-карта). Это послужило основой для последующего составления рабочих таблиц приоритета 1 и приоритета 2 (см. рабочие таблицы), которые Группа по EPDP использовала для получения данных:

- Описание проблемы / связанные вопросы устава
- Ожидаемый отчет
- Обязательно к прочтению
- Необходимые брифинги
- Правовые аспекты
- Взаимозависимые элементы
- Предлагаемые сроки и подход

Председатель Группы по EPDP также предложил ряд рабочих определений для обеспечения согласованной терминологии и единого понимания терминов, используемых в ходе обсуждений Группы по EPDP (см. рабочие определения).

После рассмотрения ряда реальных примеров использования Группа по EPDP создала набор структурных элементов, из которых могла бы состоять Система обеспечения стандартизованного доступа к данным и их раскрытия (SSAD), признавая, что решение о функциях и обязанностях различных вовлеченных сторон может зависеть как от юридических консультаций, так и от рекомендаций Европейского совета по защите данных («EDPB»).

2.3 Темы с приоритетом 1 и приоритетом 2

Для организации своей деятельности Группа по EPDP договорилась разбить темы, над которыми она работает, на два уровня приоритетности. Приоритет 1 охватывает SSAD и все непосредственно связанные с этим вопросы. Приоритет 2 включает следующие темы:

- Отображение информации аффилированных и аккредитованных провайдеров услуг сохранения конфиденциальности/регистрации через доверенных лиц
- Юридические и физические лица
- Вымарывание поля «город»
- Срок хранения данных
- Потенциальная цель для офиса технического директора ICANN
- Осуществимость использования единого обезличенного адреса электронной почты для уникальных контактных лиц
- Точность и система учета достоверности данных WHOIS

Группа по EPDP согласилась, что в первую очередь необходимо завершить обсуждение вопросов с приоритетом 1. Однако было решено, что там, где это

возможно, группа также будет стремиться параллельно работать над вопросами с приоритетом 2.

Ввиду внешних взаимозависимых элементов и ограничений по времени в этот итоговый отчет входят не все вопросы с приоритетом 2. В частности, не рассматриваются следующие вопросы:

Юридические и физические лица: Хотя этот вопрос на самом деле рассматривался в рамках фазы 2, это не привело к согласованию новых рекомендаций по политике. Материалы запрошенного исследования по этой теме были получены слишком поздно, чтобы должным образом их рассмотреть. В связи с этим и согласно рекомендациям фазы 1 EPDP, регистраторам и операторам регистратур разрешено, но не вменяется в обязанность проводить различия между владельцами доменов в зависимости от того, являются ли они физическим или юридическими лицами. Дальнейшая работа по этому вопросу (включая рассмотрение результатов проведенного корпорацией ICANN исследования под названием «Разграничение юридических и физических лиц в службе каталогов регистрационных данных доменных имен (RDDS)») находится на рассмотрении Совета GNSO.

Возможность наличия у уникальных контактных лиц единого обезличенного адреса электронной почты: Группа по EPDP получила правовые рекомендации, в которых говорится, что публикация адресов электронной почты с одинаковыми масками приводит к публикации персональных данных; это говорит о том, что широкое опубликование маскируемых адресов электронной почты в настоящее время не представляется возможным в рамках GDPR. Дальнейшая работа по этому вопросу рассматривается Советом GNSO.

2.4 Юридический комитет

Признавая сложность многих вопросов, над которыми Группе по EPDP было поручено работать на фазе 2, Группа по EPDP запросила ресурсы для привлечения внешнего юрисконсульта — компании Bird & Bird. Чтобы помочь в подготовке проектов юридических вопросов для Bird & Bird, руководство EPDP решило создать Юридический комитет, состоящий из членов Группы по EPDP с юридическим опытом.

Юридический комитет фазы 2 занимался рассмотрением вопросов, предложенных членами Группы по EPDP, чтобы гарантировать следующее:

1. вопросы действительно носят юридический характер, в отличие от вопросов политики или ее реализации;
2. вопросы сформулированы беспристрастно, избегая как предполагаемых результатов, так и позиций групп интересов;

3. вопросы уместны и своевременны для работы Группы по EPDP;
4. ограниченный бюджет для привлечения внешнего юрисконсульта используется ответственно.

Юридический комитет представил все согласованные вопросы Группе по EPDP для окончательного утверждения перед отправкой вопросов Bird & Bird, за исключением вопросов по автоматизации принятия решений.

На сегодняшний день Группа по EPDP приняла решение отправить компании Bird & Bird восемь вопросов, связанных с SSAD. Полный текст этих вопросов и основные положения юридических рекомендаций, полученных в ответ на вопросы, приведены в Приложении F.

2.5 Вопросы устава

Рассматривая вопросы устава,[2] Группа по EPDP изучила (1) вклад каждой группы в обсуждение; (2) соответствующие данные фазы 1; (3) вклад каждой группы в ответ на запрос предварительных комментариев по конкретным вопросам устава; (4) обязательные к прочтению материалы, указанные для каждой темы в рабочих таблицах, (5) комментарии на форумах общественного обсуждения, и (6) вклад юрисконсультантов Группы по EPDP (Bird & Bird).

[2] В Приложении A более подробно рассматривается связь между каждой из тем, затронутых в рекомендациях, и соответствующими вопросами устава.

3 Ответы Группы по EPDP на вопросы устава и ее рекомендации

После анализа комментариев, поступивших в период общественного обсуждения первоначального отчета и дополнения к нему Группа по EPDP представляет свои рекомендации на рассмотрение Совета GNSO. В настоящем итоговом отчете указан уровень консенсусной поддержки различных рекомендаций Группой по EPDP. Резюме:

- 11 (одиннадцать) рекомендаций получили статус «полный консенсус» (№ 1, 2, 3, 4, 11, 13, 15, 16, 17, 19 и 21).
- 3 (три) рекомендации получили статус «консенсус» (№ 7, 20 и 21).
- 6 (шесть) рекомендаций получили статус «значительная поддержка при наличии существенной оппозиции» (№ 5, 8, 9, 10, 12 и 18).
- 2 (две) рекомендации получили статус «расхождение во мнениях» (№ 6 и 14).

Дополнительные сведения об этих статусах см. в Приложении D, а также в разделе 3.6. Руководства для Рабочих групп GNSO.

Что касается рекомендаций, связанных с SSAD, Группа по EPDP считает их взаимозависимыми. Следовательно, они должны рассматриваться Советом GNSO, а затем и Правлением ICANN как единый пакет.

Примечание. На фазе 1 работы Группе по EPDP было поручено проанализировать Временную спецификацию. Временная спецификация была создана в качестве ответа на GDPR.[3] Соответственно, GDPR — единственный конкретный закон, который упоминается в этом отчете. Группа по EPDP обсудила возможность составить этот итоговый отчет таким образом, чтобы он не зависел от какого-либо конкретного закона, но пришла к выводу, что отчет выиграет от четких ссылок, облегчающих выполнение рекомендаций группы. GDPR — это региональный закон, охватывающий несколько юрисдикций; учитывая строгие критерии, которые он содержит, соблюдение этого закона с большой долей вероятности будет означать соответствие другим национальным или применимым региональным законам о защите данных. Группа по EPDP полностью поддерживает стремление ICANN к глобальному охвату, и ничто в этом отчете не отменяет базовый принцип, согласно которому стороны, связанные договорными обязательствами, могут и должны соблюдать применимые на местном уровне законодательные и нормативные акты.

[3] «В данной Временной спецификации для регистрационных данных gTLD (далее — Временная спецификация) определены временные требования, обеспечивающие регистраторам и операторам регистратур gTLD и ICANN возможность дальнейшего соблюдения существующей политики, разработанной сообществом, и контрактных требований ICANN в свете GDPR».

3.1 Система обеспечения стандартизованного доступа к закрытым регистрационным данным и их раскрытия (SSAD)

В Приложении A представлены дополнительные сведения о подходе и материалах, которые Группа по EPDP изучила для рассмотрения вопросов устава и разработки следующих рекомендаций.

По ходу дискуссий Группа по EPDP рассмотрела и централизованную модель, которая предусматривает обработку запросов и выдачу разрешения о раскрытии данных корпорацией ICANN или стороной, которой будет делегирована функция обработки данных, и децентрализованную модель, которая предусматривает обработку запросов и принятие решений о раскрытии данных сторонами, связанными договорными обязательствами (регистраторами, аккредитованными ICANN, и операторами регистратур gTLD). Группа не смогла выбрать один из двух вариантов и вместо этого предлагает гибридную модель, предусматривающую централизацию запросов и принятие решений о раскрытии данных преимущественно сторонами, связанными договорными обязательствами (на начальном этапе реализации). Гибридная модель SSAD основана на следующих общих принципах:

- Получение, аутентификация и передача запросов SSAD стороне, связанной договорными обязательствами, должны быть полностью автоматизированы, если это технически и коммерчески осуществимо и допустимо с юридической точки зрения. Решения о раскрытии данных обычно (на начальном этапе реализации) принимаются стороной, связанной договорными обязательствами, и их следует автоматизировать только в тех случаях, когда это технически и коммерчески осуществимо и допустимо с юридической точки зрения. В областях, где автоматизация не отвечает этим критериям, основной целью является стандартизация процесса принятия решений о раскрытии данных. Накопленный со временем опыт работы с запросами и ответами SSAD о раскрытии данных должен способствовать дальнейшей оптимизации и стандартизации ответов.
- Признавая необходимость корректировки функций SSAD на основе опыта, следует создать Постоянный комитет GNSO, который будет контролировать внедрение SSAD и рекомендовать целесообразные улучшения. Улучшения, рекомендованные в рамках этого процесса, не должны нарушать политику, установленную EPDP, законами о защите данных, Уставом ICANN или процедурами и рекомендациями GNSO.
- Необходимо заключить осуществимые соглашения об уровне обслуживания (SLA), но со временем, по мере накопления опыта, их, возможно, потребуется изменить.

- Ответы на запросы о раскрытии данных, независимо от того, проводится ли проверка вручную или инициированы автоматизированные ответы, отправляются соответствующей стороной, связанной договорными обязательствами, непосредственно запрашивающей стороне. Однако в SSAD должны существовать надлежащие механизмы ведения журналов, позволяющие подтвердить соблюдение SLA и политики при обработке ответов (например, центральный шлюз ДОЛЖЕН получать уведомление, когда запросы о раскрытии данных отклоняются или удовлетворяются).

Преимущества этой модели:

Единое место для подачи запросов.

- Сокращение времени и усилий, затрачиваемых подателями запросов на отслеживание отдельных контактных лиц или выполнение отдельных процедур.
- Гарантия передачи запросов напрямую ответственному лицу в каждой раскрывающей данные организации; это устраняет сомнения в отношении того, что запросы не получены или переданы для обработки некомпетентному лицу.
- Обеспечение четких возможностей информирования о месте и способе запроса закрытых регистрационных данных.
- Запросы и ответы можно отслеживать, чтобы узнать, соблюдаются ли SLA.

Стандартные формы запросов.

- Уменьшение количества запросов о раскрытии данных, которые отклоняются из-за недостатка информации.
- Повышение эффективности рассмотрения запросов раскрывающими организациями.
- Уменьшение неопределенности для подателей запросов, которые теперь должны предоставлять при отправке запросов о раскрытии стандартный/унифицированный набор данных.
- Снижение потребности в индивидуальном наборе необходимой информации для раскрывающих сторон.

Встроенный процесс аутентификации.

- Ускорение процесса проверки для раскрывающих организаций, поскольку им не нужно будет повторно проверять подателя запроса.
- Внешняя гарантия того, что податели запросов были проверены, может повысить вероятность и (или) скорость раскрытия информации.

Стандартизованный процесс проверки и ответа.

- Возможность создания стандартного формата ответа.

- Возможность создания правил, руководящих принципов и методических рекомендаций, которым раскрывающие стороны могут следовать при рассмотрении запросов и ответе на них.
- Возможность внедрения общей системы проверки ответов.
- Возможность автоматизации обработки некоторых запросов, которые еще предстоит определить, поступающих от некоторых подателей запросов, которых также предстоит определить.
- Содействие автоматизации принятия решений о раскрытии данных в некоторых сценариях.
- Ведение журнала запросов и ответов также позволяет корпорации ICANN проводить аудит действий раскрывающих информацию организаций, выявлять любые случаи систематического несоблюдения требований и принимать соответствующие принудительные меры.

Основные роли и обязанности в SSAD:

- Диспетчер центрального шлюза — роль, выполняемая корпорацией ICANN или контролируемая ею. Отвечает за управление приемом и пересылку ответственным сторонам, связанным договорными обязательствами, запросов SSAD, требующих ручной проверки. Отвечает за управление обработкой и пересылку сторонам, связанным договорными обязательствами, запросов, которые признаны пригодными для автоматизированной обработки, с целью раскрытия данных в соответствии с критериями, установленными и согласованными в настоящих рекомендациях по политике или на основе рекомендации Постоянного комитета GNSO по проверке выполнения рекомендаций по политике в отношении SSAD. Отвечает за сбор данных о запросах, ответах и принятых решениях о раскрытии данных.
- Орган по аккредитации — роль, выполняемая корпорацией ICANN или контролируемая ею. Управляющая организация, которой предоставлены официальные полномочия по «аккредитации» пользователей SSAD, то есть по проверке и подтверждению личности пользователя (указанной в удостоверении личности) и утверждений (или заявлений), связанных с удостоверением личности (содержащихся в подписанных утверждениях).
- Провайдер идентификации — отвечает за 1) проверку личности запрашивающей стороны и управление удостоверением личности, связанным с запрашивающей стороной, 2) проверку и управление подписанными утверждениями, связанными с удостоверением личности. Для целей SSAD провайдером идентификации может быть сам орган по аккредитации, либо орган по аккредитации может привлекать третьи стороны для предоставления услуг провайдера идентификации.

- Стороны, связанные договорными обязательствами, — отвечают на запросы о раскрытии данных, которые не отвечают критериям автоматизированного ответа.[4]
- Постоянный комитет GNSO по проверке выполнения рекомендаций по политике в отношении SSAD — комитет представителей сообщества ICANN, ответственный за оценку операционных проблем SSAD, возникающих в результате принятия и (или) реализации согласованной политики ICANN. Постоянный комитет GNSO предназначен для изучения данных, получаемых в результате работы SSAD, и предоставления Совету GNSO рекомендаций о наиболее полезных операционных изменениях в SSAD, которые являются исключительно мерами по реализации, в дополнение к рекомендациям, основанным на анализе влияния действующей согласованной политики в отношении работы SSAD.

Ожидается, что различные роли и обязанности будут подробно описаны и подтверждены в соответствующих соглашениях.

Ниже детализируются основные предположения и рекомендации по политике, которые Группа по EPDP выносит на рассмотрение сообщества.

3.2 Вклад Правления ICANN и корпорации ICANN

Чтобы получить информацию для обсуждений, Группа по EPDP обратилась как к Правлению ICANN, так и к корпорации ICANN, «чтобы понять позицию Правления относительно объема оперативных полномочий и уровня ответственности (в отношении принятия решений о раскрытии закрытых регистрационных данных), которые оно готовы взять на себя от имени корпорации ICANN, наряду с любыми предварительными условиями, которые могут для этого потребоваться».

Корпорация ICANN представила ответ 19 ноября 2019 года, отметив, в частности, что «корпорация ICANN выразила готовность взять на себя обязанности оператора шлюза для авторизации запросов о раскрытии данных. Как отмечалось выше, оператор шлюза не принимает решение о раскрытии данных. В предлагаемой модели провайдер авторизации будет решать, соблюдены ли критерии раскрытия информации. Если запрос авторизован и аутентифицирован, оператор шлюза будет запрашивать данные у стороны, связанной договорными обязательствами, и раскрывать соответствующий набор данных Запрашивающей стороне».[5]

[4] По умолчанию диспетчер центрального шлюза отправляет запросы о раскрытии данных регистраторам, но это не препятствует отправке диспетчером запросов о раскрытии в регистратуры при определенных обстоятельствах (более подробную информацию см. в рекомендации № 5).

[5] Обратите внимание, что описанная здесь модель не совпадает с моделью SSAD, предложенной в отчете Группы по EPDP.

Правление ICANN представило ответ 20 ноября 2019 года, отмечая, в частности, что «Правление последовательно выступает за разработку модели доступа к закрытым регистрационным данным gTLD. Если в результате 2-й фазы работы Группы по EPDP будет выработана согласованная рекомендация о том, что корпорация ICANN должна взять на себя одну или несколько операционных функций в рамках SSAD, Правление примет эту рекомендацию, если Правление не решит большинством более двух третей голосов, что такая политика не будет отвечать интересам сообщества ICANN или ICANN. Учитывая, что Правление выступает за разработку модели доступа и поддерживает диалог корпорации ICANN с EDPB по предлагаемой UAM, вполне вероятно, что Правление примет соответствующую рекомендацию EPDP».

Группа по EPDP задала корпорации ICANN ряд дополнительных уточняющих вопросов, которые вместе с ответами представлены здесь: https://community.icann.org/x/5BdIBg. Этот вклад также содержал смету расходов корпорации ICANN на предлагаемую систему стандартизованного доступа к данным и их раскрытия.

Группа по EPDP рассмотрела этот вклад, отзыв, полученный от бельгийского DPA, а также комментарии, полученные в период общественного обсуждения, для окончательного распределения ролей и ответственности в SSAD.

3.3 Исходные предположения SSAD

Для разработки своих рекомендаций по политике Группа по EPDP использовала исходные предположения, изложенные ниже. Эти исходные предположения не обязательно создают новые требования для сторон, связанных договорными обязательствами; предположения скорее призваны помочь как читателям настоящего итогового отчета, так и конечным исполнителям политики понять намерения и основополагающие допущения, которыми руководствовалась Группа по EPDP, предлагая эту модель SSAD и связанные с ней рекомендации.

- Целью SSAD является создание предсказуемого, транспарентного, эффективного и подотчетного механизма доступа к закрытым регистрационным данным и их раскрытия.
- SSAD должна соответствовать требованиям GDPR.
- SSAD должна обеспечивать возможность соблюдения этих принципов и рекомендаций по политике.
- Учитывая решения, принятые Группой по EPDP в отношении модели SSAD, рабочее предположение состоит в том, что ICANN и стороны, связанные договорными обязательствами, будут контролерами, совместно отвечающими за обработку данных. Это определение основано на фактическом анализе предлагаемой политики.

3.4 Соглашения, используемые в этом документе

Употребляемые в настоящем документе ключевые слова «ДОЛЖЕН», «НЕ ДОЛЖЕН», «ОБЯЗАТЕЛЬНО», «БУДЕТ», «НЕ БУДЕТ», «СЛЕДУЕТ», «НЕ СЛЕДУЕТ», «РЕКОМЕНДУЕТСЯ», «НЕ РЕКОМЕНДУЕТСЯ» и «МОЖЕТ» и «НЕ ОБЯЗАТЕЛЬНО» следует понимать так, как описано в документах BCP 148, RFC2119 и RFC8174.

Примечание. Принимая во внимание выбор модели Группой по EPDP и ожидая конкретной юридической консультации относительно ответственности сторон и определения инструментов контроля данных, применительно к предлагаемой модели, Группа по EPDP отмечает, что определенные утверждения в рекомендациях, могут потребовать изменения статуса с обязательного на допустимый и наоборот. (Например, «будет» на «следует», «ДОЛЖЕН» на «МОЖЕТ» и т. д.).

При ссылке на руководство по реализации Группа по EPDP учитывает, что этот дополнительный контекст и (или) уточняющая информация предоставят больше данных для реализации рекомендаций по политике. Однако Группа по EPDP отмечает, что руководство по реализации не имеет такого же веса и статуса, как текст рекомендации по определению политики.

3.5 Рекомендации Группы по EPDP в отношении SSAD

3.5.1. Определения

- **Аккредитация** — административное действие, посредством которого орган по аккредитации объявляет, что пользователь имеет право использовать SSAD в определенной конфигурации безопасности с предписанным набором мер безопасности.
- **Орган по аккредитации** — управляющая организация, которой предоставлены официальные полномочия по «аккредитации» пользователей SSAD, то есть по проверке и подтверждению личности пользователя (указанной в удостоверении личности) и утверждений (или заявлений), связанных с удостоверением личности (содержащихся в подписанных утверждениях).
- **Аудитор органа по аккредитации** — организация, отвечающая за выполнение требований органа по аккредитации в отношении аудита, как указано в рекомендации № 16 (Аудиторские проверки). Этот орган может быть независимым или, если корпорация ICANN в конечном итоге передаст роль органа по аккредитации третьей стороне, корпорация ICANN МОЖЕТ выступать в роли аудитора органа по аккредитации.
- **Аутентификация** — процесс или действие по проверке удостоверений личности и подписанных утверждений подателя запроса.

- **Авторизация** — процесс удовлетворения или отклонения запроса о раскрытии закрытых регистрационных данных.
- **Диспетчер центрального шлюза (CGM)** — роль, выполняемая корпорацией ICANN или контролируемая ею. Отвечает за управление приемом и пересылку ответственным сторонам, связанным договорными обязательствами, запросов SSAD, требующих ручной проверки. Отвечает за управление обработкой и пересылку сторонам, связанным договорными обязательствами, запросов, которые признаны пригодными для автоматизированной обработки, с целью раскрытия данных в соответствии с критериями, установленными и согласованными в настоящих рекомендациях по политике или на основе рекомендации Постоянного комитета GNSO по проверке выполнения рекомендаций по политике в отношении SSAD. Отвечает за сбор данных о запросах, ответах и принятых решениях о раскрытии данных.
- **Отмена аккредитации органа по аккредитации** — административное действие, с помощью которого корпорация ICANN аннулирует соглашение с органом по аккредитации, если эта функция передана третьей стороне, после чего ей больше не разрешается действовать в качестве органа по аккредитации.
- **Правомочное государственное учреждение** — государственное учреждение (включая органы местного самоуправления и международные правительственные организации), желающее получить доступ к закрытым регистрационным данным для реализации общественной политики в рамках своего мандата.
- **Удостоверение личности —** объект данных, который является переносимым представлением связи между идентификатором и аутентифицируемой информацией и который может быть представлен для использования при проверке личности субъекта, пытающегося получить доступ к системе. Пример: имя пользователя/пароль, учетные данные OpenID, сертификат открытого ключа X.509.
- **Провайдер идентификации** — отвечает за 1) проверку личности запрашивающей стороны и управление удостоверением личности, связанным с запрашивающей стороной, 2) проверку и управление подписанными утверждениями, связанными с удостоверением личности. Для целей SSAD провайдером идентификации может быть сам орган по аккредитации, либо орган по аккредитации может привлекать третьи стороны для предоставления услуг провайдера идентификации.
- **Податель запроса** — аккредитованный пользователь, желающий получить регистрационные данные доменного имени через SSAD.
- **Отзыв учетных данных пользователя** — событие, когда провайдер идентификации объявляет, что ранее действительные учетные данные стали недействительными.
- **Подписанное утверждение** — объект данных, который является переносимым представлением связи между удостоверением личности

и одним или несколькими утверждениями для доступа, и который может быть представлен для использования при проверке этих утверждений субъекта, пытающегося получить такой доступ. Пример: [удостоверение OAuth], сертификат атрибута X.509. Подписанные утверждения могут быть специфичными для пользователя (например, для обозначения профессиональной принадлежности или подтверждения законных процессов обработки данных) или для конкретных запросов (например, с указанием законных оснований для запроса о раскрытии).

- **Система обеспечения стандартизованного доступа к закрытым регистрационным данных gTLD и их раскрытия** (SSAD) — SSAD представляет собой совокупность сторон и компонентов, составляющих систему запроса, проверки и раскрытия информации.
- **Проверить подлинность/проверка подлинности** — проверить, доказать или установить надежность или правильность структурного компонента. (Пример: раскрывающая сторона проверяет подлинность удостоверения личности и подписанных утверждений в рамках процесса авторизации.)
- **Проверить** — проверить или подтвердить истинность или достоверность факта или значения. (Пример: провайдеры идентификации подтверждают личность запрашивающей стороны перед выдачей удостоверения личности.)
- **Проверка** — процесс изучения информации для установления истинности заявленного факта или значения.

3.5.2. Рекомендации

Recommendation #1. Аккредитация[6]

1.1. Группа по EPDP рекомендует создать или выбрать орган по аккредитации.

1.2. Группа по EPDP рекомендует, чтобы орган по аккредитации установил политику аккредитации пользователей SSAD в соответствии с рекомендациями, изложенными ниже.

1.3. Следующие рекомендации ДОЛЖНЫ быть включены в политику аккредитации:

1.3.1. SSAD ДОЛЖНА принимать запросы на доступ/раскрытие только от аккредитованных организаций или частных лиц. Однако требования к аккредитации ДОЛЖНЫ охватывать всех предполагаемых пользователей системы, в том числе людей или организации, которые делают один единственный запрос. Требования к аккредитации для постоянных и разовых пользователей системы МОГУТ отличаться.

[6] Обратите внимание, что аккредитация не относится к аккредитации/сертификации, описанным в статье 42/43 GDPR.

1.3.2. И юридические, и физические лица имеют право на аккредитацию. Индивидуальный доступ к SSAD с использованием учетных данных аккредитованной организации (например, юридических лиц) гарантирует, что физическое лицо действует с разрешения аккредитованной организации.

1.3.3. Политика аккредитации определяет единый орган по аккредитации под управлением корпорации ICANN, который отвечает за проверку, выдачу и постоянное управление удостоверениями личности и подписанными утверждениями. Орган по аккредитации ДОЛЖЕН разработать политику конфиденциальности. Орган по аккредитации МОЖЕТ сотрудничать с внешними или сторонними провайдерами идентификации, выступающими в качестве информационных служб для проверки личности и данных авторизации, которые относятся к запрашивающим аккредитацию лицам. Ответственность за обработку персональных данных, независимо от стороны, выполняющей эту обработку, остается на органе по аккредитации. Если корпорация ICANN решит передать функцию органа по аккредитации на аутсорсинг (полностью или частично), корпорация ICANN будет обязана осуществлять надзор за деятельностью стороны (сторон), которым функция или ее часть переданы на аутсорсинг. Надзор ДОЛЖЕН включать мониторинг и устранение потенциальных злоупотреблений, совершенных стороной, которой функция или ее часть была передана на аутсорсинг.

1.3.4. Решение разрешить раскрытие регистрационных данных на основании проверки удостоверения личности, подписанных утверждений и данных, как того требует рекомендация, касающаяся критериев и содержания запросов (рекомендация № 3), будет приниматься регистратором, регистратурой или диспетчером центрального шлюза, в зависимости от обстоятельств.

1.4. Требования к органу по аккредитации

1.4.1. Подтвердить личность подателя запроса: орган по аккредитации ДОЛЖЕН подтвердить личность запрашивающей стороны и создать удостоверение личности.

1.4.2. Управление подписанными утверждениями: Орган по аккредитации МОЖЕТ проверять и управлять набором динамических утверждений/заявлений, связанных с удостоверением личности подателя запроса. Эта проверка, которая может выполняться провайдером идентификации, приводит к созданию подписанного

утверждения. Подписанные утверждения[7] содержат следующую информацию:

- Утверждение относительно цели (целей) запроса
- Утверждение относительно законного основания запроса
- Утверждение, что пользователь, идентифицированный по удостоверению личности, аффилирован с соответствующей организацией
- Утверждение о соблюдении законодательства (например, хранение, защита и сохранение/удаление данных)
- Утверждение о готовности использовать раскрытые данные в указанных законных целях
- Утверждение о соблюдении мер защиты и (или) условий обслуживания; подлежит отзыву, если будет выявлен факт их нарушения
- Утверждения, касающиеся предотвращения злоупотреблений, требований аудита, разрешения споров и рассмотрения жалоб и т. д.
- Утверждения, относящиеся к подателю запроса — например, о владении товарным знаком или его регистрации
- Утверждения о доверенности, если применимо.

1.4.3. ДОЛЖЕН проверять удостоверения личности и подписанные утверждения, в дополнение к информации, содержащейся в запросе, способствовать принятию решения об удовлетворении или отклонении запроса на авторизацию в SSAD. Во избежание неправильного толкования поясняется, что наличие этих учетных данных как таковое НЕ ДОЛЖНО приводить к автоматической выдаче разрешения на доступ/раскрытие информации или делать такую выдачу обязательной. Тем не менее, допускается возможность автоматизации процесса принятия решений о предоставлении доступа/раскрытии информации при определенных обстоятельствах, если это законно.

1.4.4. Орган по аккредитации ДОЛЖЕН определить базовый «кодекс поведения»,[8] который устанавливает набор правил,

[7] Настоящим поясняется, что подписанные утверждения являются динамическими и могут изменяться в зависимости от запроса (цель, законное основание, тип, срочность и т. д.) по сравнению с удостоверением личности, которое является статическим и обычно не меняется. Подписанные утверждения используются только для связывания атрибутов с личностью. Эти атрибуты являются динамическими для каждого запроса, но при необходимости их можно проверять и управлять ими напрямую в рамках процесса аккредитации. Орган по аккредитации может заранее установить различные утверждения для определенных удостоверений личности или динамически создавать их для каждого запроса. Этот момент подлежит дополнительной проработке на этапе реализации. Орган по аккредитации может хранить несколько подписанных утверждений для каждого удостоверения личности, но податель запроса должен вызывать соответствующие утверждения для каждого запроса.

[8] Во избежание неправильного толкования поясняется, что упомянутый здесь кодекс поведения не является ссылкой на Кодекс поведения, описанный в GDPR. Упомянутый здесь кодекс поведения относится к набору правил и стандартов, которым должен следовать орган по аккредитации.

способствующих правильному применению законов о защите данных, таких как GDPR, в том числе:

- Четкое и краткое разъяснение.
- Конкретные рамки, которые определяют охватываемые операции обработки (в SSAD основное внимание будет уделяться операции раскрытия информации).
- Механизм, позволяющий контролировать соблюдение положений.
- Определение аудитора органа по аккредитации (также известного как орган мониторинга) и определение механизмов, которые позволят этому органу выполнять свои функции.
- Описание того, в каком объеме проведены «консультации» с заинтересованными сторонами.

1.4.5. Орган по аккредитации ДОЛЖЕН разработать политику конфиденциальности при обработке персональных данных, которую он обязуется соблюдать, а также условия обслуживания своих аккредитованных пользователей (как указано в рекомендации № 11).

1.4.6. Разработать базовую процедуру подачи заявки: Орган по аккредитации ДОЛЖЕН разработать единую базовую процедуру подачи заявки и сопутствующие требования для всех провайдеров идентификации (если применимо) и всех заявителей, запрашивающих аккредитацию, в том числе:

i. Сроки аккредитации
ii. Определение квалификационных требований к аккредитованным пользователям
iii. Проверка личности, процедуры
iv. Политика управления удостоверениями личности: срок действия/истечение срока, периодичность обновления, свойства безопасности (политика/надежность пароля или ключа) и т. д.
v. Процедуры отзыва удостоверения личности: обстоятельства отзыва, механизмы отзыва и т. д. (см. также раздел «Отзыв аккредитации пользователя и злоупотребления» ниже)
vi. Управление подписанными утверждениями: срок действия/истечение срока, периодичность обновления и т. д.
vii. ПРИМЕЧАНИЕ: может возникнуть необходимость ввести требования, выходящие за рамки перечисленных выше базовых требований, для определенных категорий подателей запросов.

1.4.7. Определить процесс разрешения споров и подачи жалоб: Орган по аккредитации ДОЛЖЕН определить процесс разрешения споров и подачи жалоб с целью оспорить действия органа по аккредитации. Установленный процесс ДОЛЖЕН включать сдерживающие и уравновешивающие силы.

1.4.8. Аудиторские проверки: Орган по аккредитации ДОЛЖЕН регулярно проходить аудиторскую проверку. Если будет обнаружено, что орган по аккредитации нарушает политику и требования аккредитации,

ему будет предоставлена возможность исправить нарушение, но в случае систематических нарушений необходимо выбрать или создать новый орган по аккредитации. Кроме того, аккредитованные организации ДОЛЖНЫ регулярно проходить аудит на соответствие политике и требованиям аккредитации; (примечание: подробная информация о требованиях к аудиту как для органа по аккредитации, так и для любых провайдеров идентификации, которых он может использовать, представлена в рекомендации № 16 по аудиту).

1.4.9. Группы пользователей: Орган по аккредитации МОЖЕТ создавать группы/категории пользователей для облегчения процесса аккредитации, поскольку все податели запросов должны быть аккредитованы, а аккредитация будет включать проверку личности.

1.4.10. Отчетность: Орган по аккредитации ДОЛЖЕН публично и регулярно сообщать количество полученных запросов на аккредитацию, утвержденных запросов на аккредитацию и ее продление, отказов в аккредитации, отозванных аккредитаций, полученных жалоб и информировать о провайдерах идентификации, с которыми он работает. См. также рекомендацию № 17 по отчетности.

1.4.11. Продление срока действия: Орган по аккредитации ДОЛЖЕН установить сроки и требования для продления аккредитации.

1.4.12. Подтверждение пользовательских данных: Орган по аккредитации ДОЛЖЕН периодически (например, ежегодно) отправлять аккредитованным пользователям напоминания о необходимости подтверждения пользовательских данных и напоминать аккредитованным пользователям о необходимости обновлять информацию, требуемую для аккредитации. Изменения в этой требуемой информации МОГУТ привести к необходимости повторного получения аккредитации.

1.5. Отзыв аккредитованного пользователя

1.5.1. Отзыв в контексте SSAD означает, что орган по аккредитации может аннулировать статус аккредитованного пользователя SSAD.[9] Неполный список ситуаций, когда может применяться отзыв, включает 1) нарушение аккредитованным пользователем любых применимых мер безопасности или условий обслуживания, 2) изменение принадлежности аккредитованного пользователя, 3) нарушение требований к хранению/уничтожению данных или 4) исчезновение предпосылок для аккредитации.

[9] Настоящим поясняется, что юридическое лицо не будет автоматически лишено аккредитации за одно действие индивидуального пользователя, чья аккредитация связана с аккредитацией юридического лица, но юридическое лицо может понести ответственность за действия такого индивидуального пользователя.

1.5.2. Орган по аккредитации ДОЛЖЕН создать механизм апелляции, позволяющий аккредитованному пользователю оспорить решение об отзыве статуса аккредитованного пользователя в течение определенного срока, который будет установлен органом по аккредитации. Однако на время рассмотрения апелляции действие статуса аккредитованного пользователя будет приостановлено. О результатах рассмотрения апелляции НЕОБХОДИМО сообщать с соблюдением принципов транспарентности.

1.5.3. SSAD ДОЛЖНА обеспечить наличие механизма информирования о нарушении аккредитованным пользователем каких-либо мер безопасности или условий обслуживания.[10] Сообщения ДОЛЖНЫ передаваться в орган по аккредитации для обработки. Для выявления злоупотреблений орган по аккредитации МОЖЕТ также получать информацию от других сторон.

1.5.4. Политика отзыва для физических/юридических лиц ДОЛЖНА включать ступенчатые штрафные санкции; они будут детализированы в ходе реализации с учетом того, как ступенчатые штрафные санкции применяются в других областях ICANN. Другими словами, не каждое нарушение правил системы приведет к отзыву аккредитации; тем не менее, отзыв МОЖЕТ произойти, если орган по аккредитации определит, что аккредитованное физическое или юридическое лицо существенно нарушило условия своей аккредитации и не смогло устранить нарушение, на основании: i) полученной и подтвержденной жалобы третьей стороны; ii) результатов аудита или расследования, проведенного органом по аккредитации или аудитором; iii) любого неправильного использования предоставленных привилегий или злоупотребления ими; iv) неоднократных нарушений политики аккредитации; v) результатов аудита или расследования DPA.

1.5.5. При наличии модели или практики злоупотреблений со стороны физического/юридического лица, действие учетных данных этого физического/юридического лица МОЖЕТ быть приостановлено или прекращено в рамках ступенчатых штрафных санкций.

1.5.6. Такой отзыв ДОЛЖЕН препятствовать восстановлению аккредитации в будущем при отсутствии особых обстоятельств, представленная информация о которых удовлетворит орган по аккредитации.

1.5.7. Во избежание разночтений настоящим поясняется, что аннулирование аккредитации не препятствует подаче физическими или юридическими лицами в будущем запросов в соответствии с методом доступа, предусмотренным в рекомендации 18

[10] Примечание: злоупотребление SSAD со стороны аккредитованного пользователя рассматривается в рекомендации № 13.

(Обоснованные запросы на законное раскрытие информации) отчета по фазе 1 EPDP.

1.6. Отмена авторизации провайдеров идентификации

1.6.1. Отмена авторизации провайдеров идентификации: Процедуры проверки провайдеров идентификации ДОЛЖНЫ включать ступенчатые штрафные санкции. Другими словами, не каждое нарушение политики приведет к отмене авторизации; тем не менее, отмена авторизации может произойти, если было установлено, что провайдер идентификации существенно нарушил условия своего контракта и не смог устранить проблему, на основании: i) полученной жалобы третьей стороны; ii) результатов аудита или расследования, проведенного аудитором по аккредитации или аудитором; iii) любого неправильного использования предоставленных привилегий или злоупотребления ими; iv) неоднократных нарушений политики аккредитации. В зависимости от характера и обстоятельств, приведших к отмене авторизации провайдера идентификации, его оставшиеся учетные данные частично или полностью могут быть отозваны или переданы другому провайдеру идентификации.

1.6.2. Орган по аккредитации ДОЛЖЕН создать механизм апелляции, позволяющий провайдеру идентификации оспорить решение об отмене авторизации провайдера идентификации. Однако на время рассмотрения апелляции действие статуса провайдера идентификации будет приостановлено. О результатах рассмотрения апелляции НЕОБХОДИМО сообщать с соблюдением принципов транспарентности.

1.7. Дополнительные соображения касательно аккредитованных юридических и физических лиц:

1.7.1. ДОЛЖНЫ согласиться:

1.7.1.1. Использовать данные только в законных целях.

1.7.1.2. Принять условия обслуживания, в которых описано законное использование данных.

1.7.1.3. Предотвращать злоупотребление полученными данными.

1.7.1.4. Сотрудничать для выполнения всех аудиторских или информационных запросов при проведении аудита.

1.7.1.5. Подлежать лишению аккредитации, если будет установлен факт неправильного использования данных или нарушения политики/требований аккредитации.

1.7.1.6. Хранить, защищать и удалять регистрационные данные gTLD в соответствии с действующим законодательством.

1.7.2. Сохранять регистрационные данные gTLD только до тех пор, пока это необходимо для достижения цели, указанной в запросе о раскрытии данных.

1.7.3. Количество запросов SSAD, которые могут быть отправлены в течение определенного периода времени, НЕ ДОЛЖНО быть ограничено, за исключением случаев, когда аккредитованная организация представляет очевидную угрозу SSAD или когда могут быть введены иные ограничения в соответствии с настоящими рекомендациями (например, в соответствии с рекомендациями 1.5(d) и 13(b)). Разумеется, при отправке ответов SSAD могут существовать ограничения, обусловленные пропускной способностью и скоростью.

1.7.4. ДОЛЖНЫ поддерживать актуальность информации, необходимой для аккредитации и проверки, и незамедлительно информировать орган по аккредитации об изменениях в этой информации. Любые изменения МОГУТ привести к повторной аккредитации или повторной проверке определенной части предоставленной информации.

Руководство по реализации

1.8. В отношении аккредитации Группа по EPDP дает следующие указания по реализации, понимая, что дальнейшие подробности будут определены на этапе реализации:

1.8.1. Подходящие авторитетные и хорошо зарекомендовавшие себя организации могут поддерживать орган по аккредитации в качестве провайдеров идентификации. Если какие-либо уважаемые и хорошо зарекомендовавшие себя организации намерены сотрудничать с органом по аккредитации, ДОЛЖНА проводиться надлежащая проверка, как описано в пункте 1.3 (f) выше.

1.8.2. Примеры дополнительной информации, которую орган по аккредитации или провайдер идентификации МОЖЕТ затребовать у лица, подающего заявку на аккредитацию, могут включать следующее:

- регистрационный номер предприятия и название органа, выдавшего этот номер (если лицо, подающее заявку на аккредитацию, является юридическим лицом);
- информация, подтверждающая право собственности на товарный знак.[11]

[11] Настоящим поясняется, что поставщики услуг и (или) юристы, действующие от имени владельцев товарных знаков, также имеют право на аккредитацию. Однако такие поставщики услуг и (или) юристы действуют от имени (на законных основаниях) владельца товарного знака. Если такие поставщики услуг и (или) юристы нарушают правила SSAD, необходимо сообщать об этом раскрывающим данные организациям, и необходимо

1.9. Аудит и ведение журналов органом по аккредитации и провайдерами идентификации

1.9.1. Действия по аккредитации/проверке (такие как запрос на аккредитацию, информация, на основании которой было принято решение об аккредитации или проверке личности) будут регистрироваться органом по аккредитации и провайдерами идентификации.

1.9.2. Зарегистрированные данные ДОЛЖНЫ быть раскрыты или иным образом предоставлены для проверки органом по аккредитации или провайдером идентификации только в тех случаях, когда раскрытие считается необходимым для а) выполнения или соблюдения применимых юридических обязательств органа по аккредитации или провайдера идентификации; б) проведения аудита в соответствии с данной политикой или с) для поддержки нормального функционирования SSAD и политики аккредитации.

См. также рекомендации по аудиту и ведению журналов.

1.10. Проверка Корпорации ICANN следует использовать свой опыт в других областях, где требуется проверка, таких как аккредитация регистраторов, чтобы на фазе реализации выдвинуть предложение о проверке личности подателя запроса.

1.11. Периоды подтверждения аккредитации. В качестве передовой практики можно рассмотреть период подтверждения аккредитации и требования к регистраторам (в настоящее время — 5 лет). Во избежание разночтений настоящим поясняется: ничто не запрещает органу по аккредитации затребовать дополнительную документацию при продлении аккредитации.

1.12. Ожидается, что аккредитованная организация разработает соответствующую политику и процедуры, обеспечивающие надлежащее использование отдельными лицами своих полномочий. Каждый пользователь должен быть аккредитован, но аккредитация пользователя, действующего от имени организации, должна быть привязана к аккредитации его организации.

ясно понимать, что такое нарушение может учитываться в будущем при раскрытии данных владельцу товарного знака, от имени которого действует агент. Привлечение различных сторонних агентов не может использоваться как средство избежать прошлых санкций за неправильное использование SSAD.

Recommendation #2. Аккредитация государственных организаций

2.1. Цель аккредитации

SSAD ДОЛЖНА предоставить доступ в разумных пределах к регистрационным данным организациям, которым необходим доступ к этим данным для выполнения своих задач в рамках общественной политики. Ввиду их обязательств в соответствии с применимыми правилами защиты данных, окончательная ответственность за предоставление доступа к закрытым регистрационным данным остается за стороной, которая считается контролером обработки этих регистрационных данных, составляющих персональные данные.

Разработка и реализация процедуры аккредитации, которая конкретно применяется к государственным организациям, будет способствовать принятию необходимых решений сторонами, связанными договорными обязательствами, перед предоставлением доступа к закрытым регистрационным данным определенной организации или перед автоматизированной обработкой решений диспетчера центрального шлюза о раскрытии данных, если применимо. Эта процедура аккредитации может предоставить контролерам данных информацию, необходимую для оценки и принятия решения о раскрытии данных.

2.2. Правомочность

Аккредитация правительством страны/территории или его уполномоченным органом[12] будет доступна различным правомочным государственным учреждениям,[13] которым требуется доступ к закрытым регистрационным данным для выполнения своей задачи в рамках общественной политики. К таким учреждениям относятся:

- Правоохранительные органы по гражданским и уголовным делам
- Органы защиты данных и регулирующие органы
- Судебные органы
- Организации по защите прав потребителей, перед которыми по закону или по поручению государственного органа поставлена задача в области общественной политики
- Органы кибербезопасности, перед которыми по закону или по поручению государственного органа поставлена задача в области общественной политики, включая национальные группы быстрого реагирования на нарушения компьютерной безопасности (CERT)

[12] Соображения по поводу реализации: таким органом могла бы быть международная правительственная организация.

[13] Межправительственные организации (МПО) также имеют право на аккредитацию согласно рекомендации № 2. МПО, которая хочет получить аккредитацию, ДОЛЖНА подать заявку на аккредитацию через орган по аккредитации страны места нахождения.

2.3. Определение правомочности

Правомочные государственные организации — это те, которым требуется доступ к закрытым регистрационным данным для выполнения своей задачи в рамках общественной политики в соответствии с применимыми законами о защите данных. Правомочность организации определяется национальным/территориальным органом по аккредитации. Это определение правомочности не влияет на окончательную ответственность стороны, связанной договорными обязательствами, по определению того, следует ли раскрывать персональные данные после запроса закрытых регистрационных данных или со стороны диспетчера центрального шлюза в случае запросов, которые соответствуют критериям автоматизированной обработки решений о раскрытии данных, если применимо.

2.4. Требования к государственному органу аккредитации

Требования к государственной аккредитации ДОЛЖНЫ соответствовать требованиям, изложенным в рекомендации 1.3.

Кроме того, требования ДОЛЖНЫ быть перечислены и доступны правомочным государственным органам. Несоблюдение этих требований может привести к лишению аккредитации органа по аккредитации корпорацией ICANN.

2.5. Процедура аккредитации

Аккредитацию ДОЛЖЕН предоставлять утвержденный орган по аккредитации. Таким органом может быть национальное/территориальное государственное учреждение (например, министерство), либо полномочия могут быть делегированы межправительственной организации. Этому органу СЛЕДУЕТ публиковать требования к аккредитации и проводить процедуру аккредитации правомочных государственных органов.

2.5.1. Аккредитация подчеркивает обязанности лица, запрашивающего данные (получателя), который несет ответственность за соблюдение закона.
2.5.2. Аккредитация будет ориентирована на соблюдение требований закона, например требований в отношении срока хранения данных, безопасного хранения, организационных средств управления данными и уведомлений о нарушениях.
2.5.3. Продление аккредитации, ведение журналов, аудит, жалобы и аннулирование аккредитации будут рассматриваться в соответствии с рекомендацией 1.

Руководство по реализации.

2.6. Для участия в SSAD государственной организации требуется аккредитация. Неаккредитованные государственные организации могут запрашивать данные за рамками SSAD. При этом у сторон, связанных договорными обязательствами, должны быть процедуры, обеспечивающие доступ к данным в разумных пределах.

2.7. Аккредитованные пользователи должны будут соблюдать меры безопасности, установленные политикой (см. также рекомендацию № 11 «Положения и условия SSAD»). Это не нанесет ущерба организации в плане соблюдения гарантий, предусмотренных ее национальным законодательством.

2.8. Аккредитованным организациям СЛЕДУЕТ предоставлять подробные сведения, которые помогут сторонам, связанным договорными обязательствами, принимать решение о раскрытии данных, например, любой применимый местный закон, относящийся к запросу.

Recommendation #3. Критерии и содержание запросов

3.1. Цель этой рекомендации — способствовать стандартизации предоставления запрошенных элементов данных, включая любые подтверждающие документы.

3.2. Группа по EPDP рекомендует ОБЯЗАТЕЛЬНО включать в каждый запрос SSAD всю информацию, необходимую для принятия решения о раскрытии данных, в том числе следующие сведения:

3.2.1. Доменное имя, относящееся к запросу на доступ к данным и их раскрытие.

3.2.2. Идентификационные данные подателя запроса и информацию о нем, включая информацию о личности и подписанных утверждениях, как указано в разделах 1.4a) и 1.4b) рекомендации № 1.[14]

3.2.3. Информация о юридических правах подателя запроса, связанных с конкретным запросом, и законном интересе или другом законном основании и (или) обосновании запроса (например, каков законный интерес или иное законное основание; почему у подателя запроса возникла необходимость запросить эти данные).

3.2.4. Подтверждение того, что запрос сделан добросовестно и полученные данные (если таковые имеются) будут

[14] Все стороны, участвующие в SSAD, должны будут учитывать возможные требования к трансграничной передаче данных.

обрабатываться на законных основаниях и только в соответствии с целью, указанной в пункте (c).

3.2.5. Список элементов данных, запрошенных подателем запроса, с указанием причин, по которым запрошенные элементы данных необходимы для цели запроса.

3.2.6. Тип запроса (например, срочный — см. также рекомендацию № 6 «Уровни приоритета, конфиденциальность» и рекомендацию № 12 «Требования к раскрытию данных»).

3.3. Диспетчер центрального шлюза[15] ДОЛЖЕН подтвердить, что вся необходимая информация предоставлена. Если диспетчер центрального шлюза обнаружит, что запрос неполный, он ДОЛЖЕН уведомить об этом подателя запроса с указанием того, какие обязательные данные отсутствуют, и предоставить подателю запроса возможность дополнить свой запрос. Необходимо исключить возможность отправки подателем запроса неполного запроса.

Руководство по реализации

Согласно ожиданиям Группы по EPDP:

3.4. Каждый запрос должен содержать данные, связанные с информацией, подробно описанной в разделе 3.2 выше. Хотя механизм сбора и включения этих данных в запрос (будь то веб-форма, API или аналогичный механизм) не указан в настоящей политике, можно рассмотреть вариант предварительного заполнения полей, установки флажков и (или) раскрывающихся меню. Однако использование предварительно заполненных полей, флажков или раскрывающихся меню не должно исключать возможность подателя запроса отправлять ответы в свободной форме.

3.5. Запросы должны быть на английском языке, если только сторона, связанная договорными обязательствами, которая получает запрос, не укажет, что желает получить запрос и (или) подтверждающие документы на другом языке (языках)**.**

3.6. Подписанное утверждение может обеспечивать выполнение одного или нескольких требований, перечисленных выше.

[15] См. определение в разделе 3.5.1 «Определения».

Recommendation #4. Подтверждение получения и дальнейшая передача запроса о раскрытии данных

4.1. Подтверждение получения

4.1.1. После подтверждения того, что запрос синтаксически правильный и все обязательные поля заполнены, диспетчер центрального шлюза ДОЛЖЕН немедленно подтвердить его получение и одновременно передать запрос о раскрытии данных[16] ответственной стороне, связанной договорными обязательствами.

4.1.2. В ответ диспетчера центрального шлюза подателю запроса СЛЕДУЕТ также включать информацию о последующих шагах, о возможностях получения общедоступных регистрационных данных, а также об ожидаемых сроках в соответствии с SLA, описанными в рекомендации № 10.

4.2. Передача запроса о раскрытии данных

4.2.1. По умолчанию диспетчер центрального шлюза ДОЛЖЕН передавать запрос о раскрытии данных регистратору записи. Однако если диспетчеру центрального шлюза известно о каких-либо обстоятельствах, оцениваемых в соответствии с этими рекомендациями, которые требуют отправки запроса о раскрытии данных соответствующему оператору регистратуры, диспетчер центрального шлюза МОЖЕТ передать запрос о раскрытии данных соответствующему оператору регистратуры, при условии, что оператор регистратуры будет проинформирован о причинах, требующих такой передачи запроса. Податель запроса ДОЛЖЕН иметь возможность сообщать о таких обстоятельствах диспетчеру центрального шлюза. Однако последний ДОЛЖЕН самостоятельно оценить, требует ли указанное обстоятельство передачи запроса о раскрытии информации соответствующему оператору регистратуры. Настоящим поясняется, что ни одно из положений данной рекомендации не мешает подателю запроса напрямую обратиться (за рамками SSAD) к соответствующему оператору регистратуры с запросом о раскрытии данных.

Руководство по реализации

Согласно ожиданиям Группы по EPDP:

4.3. Подтверждение получения будет содержать «номер запроса» или аналогичное средство для облегчения взаимодействия между подателем запроса и SSAD; детали будут проработаны при реализации.

4.4. Диспетчер центрального шлюза передает запрос о раскрытии данных, а также необходимые и достаточные сведения о подателе запроса стороне, связанной договорными обязательствами. Если это касается запросов о раскрытии данных, для которых применяется автоматизированная обработка решений о раскрытии данных (см. рекомендацию «Автоматизация»), передача запроса о раскрытии данных и всех необходимых сведений может производиться одновременно, когда диспетчер центрального шлюза будет давать указание стороне, связанной договорными обязательствами, автоматически раскрыть запрашиваемые данные подателю запроса.

Recommendation #5. Требования к ответам

5.1. Для диспетчера центрального шлюза:[17]

5.1.1. В рамках передачи запроса ответственной стороне, связанной договорными обязательствами, диспетчер центрального шлюза МОЖЕТ давать рекомендации стороне, связанной договорными обязательствами, следует ли раскрывать информацию или нет.

5.2. Для сторон, связанных договорными обязательствами:

5.2.1. Сторона, связанная договорными обязательствами, МОЖЕТ выполнить рекомендацию диспетчера центрального шлюза, но не обязана это делать. Если сторона, связанная договорными обязательствами, отказывается следовать рекомендации диспетчера центрального шлюза, она ДОЛЖНА сообщить причины невыполнения этой рекомендации, чтобы диспетчер центрального шлюза мог наращивать свои знания и улучшать будущие рекомендации по раскрытию информации.

5.2.2. При отсутствии исключительных обстоятельств ДОЛЖНА дать ответ на запрос о раскрытии данных без неоправданной задержки. К таким исключительным обстоятельствам МОЖЕТ относиться общее количество полученных запросов, если оно значительно превышает установленные SLA.[18] На запросы SSAD, отвечающие

[17] Обратите внимание, что требования к запросам о раскрытии данных, которые отвечают критериям автоматизированного принятия решений о раскрытии данных, изложены в рекомендации № 9.

[18] Для получения дополнительной информации о том, что считается злоупотреблением SSAD, см. рекомендацию № 12.

критериям автоматического ответа, должен быть отправлен автоматический ответ. Для запросов, не отвечающих критериям автоматического ответа, ответ ДОЛЖЕН предоставляться в соответствии с SLA, описанными в рекомендации по SLA.

5.2.3. Ответы на отклоненные (полностью или частично) запросы о раскрытии данных ДОЛЖНЫ содержать обоснование, достаточное для того, чтобы податель запроса понял объективные причины принятого решения, в том числе, например, анализ и разъяснение того, как проводилась проверка сбалансированности интересов[19] (если применимо). Кроме того, сторона, связанная договорными обязательствами, МОЖЕТ включать в свой ответ информацию о способе получения общедоступных регистрационных данных.

5.2.4. Если сторона, связанная договорными обязательствами, установит, что раскрытие информации повлечет нарушение применимых законов или противоречит этим рекомендациям по политике, сторона, связанная договорными обязательствами, ДОЛЖНА задокументировать обоснование и сообщить эту информацию подателю запроса, и, по запросу, корпорации ICANN.

5.3. Если податель запроса считает, что его запрос был отклонен в нарушение процедурных требований настоящей политики, МОЖЕТ быть подана жалоба в корпорацию ICANN. Корпорация ICANN ДОЛЖНА расследовать жалобы, касающиеся запросов о раскрытии данных, в рамках своих процедур контроля за соблюдением обязательств.

5.4. Корпорация ICANN ДОЛЖНА обеспечить наличие механизма оповещения, с помощью которого податели запросов и субъекты данных, чьи данные были раскрыты, могут уведомить корпорацию ICANN о том, что считают разглашение или неразглашение данных результатом систематических злоупотреблений стороны, связанной договорными обязательствами. Этот механизм оповещения не является механизмом апелляции — чтобы оспорить разглашение или неразглашение данных, затронутым сторонам следует использовать доступные механизмы разрешения споров, такие как суды или органы по защите данных — но это должно способствовать получению отделом по контролю исполнения договорных обязательств ICANN заявлений о систематическом несоблюдении требований данной политики, что должно повлечь соответствующие принудительные меры.

[19] В соответствии с рекомендацией № 6 необходимо следить за тем, чтобы в этом объяснении подателю запроса не раскрывались никакие персональные данные.

Руководство по реализации

5.5. Ожидается, что информация, полученная в результате применения механизма оповещения, также будет включаться в отчет о состоянии дел с внедрением SSAD (см. рекомендацию № 18), чтобы способствовать дальнейшему рассмотрению возможных средств борьбы со злоупотреблениями.

5.6. Группа по EPDP не ожидает, что диспетчер центрального шлюза будет давать свою рекомендацию с первого дня, поскольку понятно, что необходимо наработать опыт, прежде чем диспетчер центрального шлюза сможет давать такую рекомендацию стороне, связанной договорными обязательствами. Ожидается, что рекомендация будет даваться в автоматизированном режиме на основе информации, содержащейся в запросе, сведений о подателе запроса и истории его запросов.

Recommendation #6. Уровни приоритета

6.1. Группа по EPDP рекомендует, чтобы диспетчер центрального шлюза использовал как минимум следующие три (3) уровня приоритета, которые податель запроса может выбрать при отправке запросов через SSAD. Уровень приоритета определяет срочность, с которой запрос о раскрытии данных должен быть обработан стороной, связанной договорными обязательствами:

6.1.1. **Приоритет 1** — срочные запросы — критерии определения срочных запросов ограничиваются следующими обстоятельствами: непосредственная угроза для жизни, серьезные телесные повреждения, критическая инфраструктура (онлайн и офлайн) или эксплуатация детей. Во избежание разночтений настоящим поясняется, что приоритет 1 не ограничивается запросами правоохранительных агентств.

6.1.2. **Приоритет 2** — административные процедуры ICANN — запросы о раскрытии данных, являющиеся результатом административных процедур в соответствии с контрактными требованиями ICANN или существующими согласованными политиками, например, запросы в рамках проверок UDRP и URS.[20]

6.1.3. **Приоритет 3** — все остальные запросы.

6.2. Для запросов с уровнем приоритета 3 податели запросов ДОЛЖНЫ иметь возможность указать, что запрос о раскрытии данных касается проблемы

[20] Настоящим поясняется, что, согласно ожиданиям, этот уровень приоритета будет присваиваться только запросам одобренных ICANN поставщиков услуг по разрешению споров или их сотрудников в контексте административных процедур ICANN.

защиты потребителей (фишинг, вредоносное ПО или мошенничество), и в этом случае сторона, связанная договорными обязательствами, ДОЛЖНА отдать приоритет такому запросу относительно других запросов с уровнем приоритета 3. Постоянное злоупотребление этим критерием может привести к лишению подателя запроса аккредитации.

6.3. Сторона, связанная договорными обязательствами:

- МОЖЕТ переназначить уровень приоритета во время рассмотрения запроса. Например, при рассмотрении запроса вручную сторона, связанная договорными обязательствами, МОЖЕТ заметить, что, хотя установлен уровень приоритета 2 (административная процедура ICANN), запрос не содержит доказательств, подтверждающих наличие административной процедуры ICANN, например зарегистрированного дела UDRP, и, соответственно, запросу необходимо присвоить уровень приоритета 3.
- ДОЛЖНА сообщать о любом изменении категории диспетчеру центрального шлюза и подателю запроса.

6.4. Группа по EPDP рекомендует, чтобы SSAD была ОБЯЗАНА поддерживать «срочные» запросы к SSAD о раскрытии данных, к которым применяются следующие требования:

6.4.1. Злоупотребление срочными запросами: Нарушения правил использования срочных запросов SSAD повлекут за собой ответные меры со стороны диспетчера центрального шлюза, призванные гарантировать, что требования к срочным запросам SSAD известны и выполняются (при первом нарушении). Однако повторные нарушения могут привести к тому, что диспетчер центрального шлюза приостановит возможность отправки срочных запросов через SSAD.

6.4.2. Стороны, связанные договорными обязательствами, ДОЛЖНЫ назначить специальное контактное лицо для работы со срочными запросами SSAD. Контактные данные этого лица могут храниться и использоваться диспетчером центрального шлюза в обстоятельствах, когда запрос SSAD помечен как срочный.

6.5. Группа по EPDP рекомендует ОБЯЗАТЬ стороны, связанные договорными обязательствами, публиковать свои стандартные часы работы, рабочие дни и соответствующий часовой пояс на портале SSAD.

Руководство по реализации

6.6 Для справки см. документ Концепция порядка действий операторов регистратур при возникновении угроз безопасности, в котором

отмечается: «*Присвоение запросу при начальной оценке статуса «первоочередного» должно говорить само за себя; не требуется уникальных умений, чтобы определить связь данного запроса с общественной безопасностью. «Первоочередными» следует считать прямые угрозы человеческой жизни и ключевой инфраструктуре или эксплуатацию детей».*

6.7 Ключевая инфраструктура — это физические и кибернетические системы, которые жизненно важны, поскольку их неработоспособность или уничтожение окажут серьезное пагубное воздействие на физическую или экономическую безопасность, здоровье или безопасность населения.

6.8 См. также рекомендацию № 10, в которой содержатся дополнительные сведения о требованиях к срочному запросу SSAD.

Как определяется приоритет?
Приоритет — это код, присваиваемый запросам о раскрытии данных, который предполагает, что обработка будет происходить в соответствии с согласованным, оптимальным целевым сроком ответа.

Кто устанавливает приоритет?
Первоначальный приоритет запроса о раскрытии данных устанавливает податель запроса с использованием уровней приоритета, определенных данной политикой. При выборе приоритета диспетчер центрального шлюза четко определяет критерии, применимые к срочному запросу, и возможные последствия злоупотребления этим уровнем приоритета.

Что произойдет, если необходимо изменить приоритет?
Возможно, что при рассмотрении запроса потребуется переназначить первоначально установленный приоритет. Например, при рассмотрении запроса вручную сторона, связанная договорными обязательствами, МОЖЕТ заметить, что, хотя установлен уровень приоритета 2 (UDRP/URS), запрос не содержит доказательств, подтверждающих наличие зарегистрированного дела UDRP, и, соответственно, запросу необходимо присвоить уровень приоритета 3. О любом изменении приоритета ТРЕБУЕТСЯ сообщать диспетчеру центрального шлюза и подателю запроса. После получения от диспетчера центрального шлюза неавтоматизированного запроса о раскрытии данных сторона, связанная договорными обязательствами, должна определить, следует ли раскрывать закрытые данные. В пределах указанного выше срока ответа сторона, связанная договорными обязательствами, ДОЛЖНА ответить на запрос.

Recommendation #7. Цели подателя запроса

7.1. Группа по EPDP рекомендует следующее:

7.1.1. Податели запросов ДОЛЖНЫ подавать запросы о раскрытии данных для конкретных целей, в том числе: (i) обеспечение соблюдения уголовного законодательства, национальной или общественной безопасности, (ii) расследования, не связанные с правоохранительными органами, и гражданские иски, включая нарушение прав на интеллектуальную собственность и иски UDRP и URS, (iii) защита потребителей, предотвращение злоупотреблений и безопасность сетей и (iv) обязательства, применимые к регулируемым организациям.[21] Податели запросов МОГУТ также подавать запросы для проверки данных с согласия владельца зарегистрированного имени (RNH), которое было получено подателем запроса (при этом вся полнота ответственности лежит на подателе запроса), например для подтверждения заявления RNH о праве собственности на доменное имя, или на основании договора с подателем запроса.

7.1.2. Утверждение о наличии одной из этих конкретных целей не гарантирует доступ во всех случаях, но будет зависеть от оценки конкретного запроса, соблюдения всех применимых требований политики и законного основания запроса.

Recommendation #8. Авторизация сторон, связанных договорными обязательствами.

Настоящим поясняется, что эта рекомендация относится к запросам о раскрытии данных, которые передаются на рассмотрение стороны, связанной договорными обязательствами. Эти требования НЕ применяются к запросам о раскрытии данных, которые отвечают критериям автоматизированной обработки решений о раскрытии данных, как описано в рекомендации № 9, независимо от того, требуется ли автоматизированная обработка или она выполняется по запросу стороны, связанной договорными обязательствами. Эта рекомендация не лишает стороны, связанные договорными обязательствами, возможности проводить различие между владельцами доменов на основе географического положения, как указано в рекомендации № 16 (из фазы 1 EPDP), а также не лишает стороны, связанные договорными обязательствами, возможности проводить различие между юридическими и физическими лицами в соответствии с рекомендацией № 17 (из фазы 1 EPDP) при выполнении этой конкретной рекомендации.

[21] Например, Директива ЕС по безопасности сетей и информационных систем (известная как Директива NIS) налагает определенные обязательства на поставщиков цифровых услуг и операторов основных услуг.

Общие требования

Сторона, связанная договорными обязательствами

8.1. ДОЛЖНА рассматривать каждый запрос индивидуально, а не массово, независимо от того, выполняется ли автоматическая или полноценная проверка, и НЕ ДОЛЖНА раскрывать данные только на основании категории аккредитованного пользователя.

8.2. МОЖЕТ передавать обязанности по авторизации стороннему провайдеру, но сторона, связанная договорными обязательствами будет нести конечную ответственность за соблюдение применимых требований.

8.3. ДОЛЖНА определять собственное законное основание для обработки, связанной с решением о раскрытии данных.[22] Податель запроса будет иметь возможность указывать законное основание, исходя из которого он ожидает, что сторона, связанная договорными обязательствами, раскроет запрошенные данные; однако во всех случаях, когда сторона, связанная договорными обязательствами, несет ответственность за принятие решения о раскрытии, сторона, связанная договорными обязательствами, ДОЛЖНА вынести окончательное решение о наличии соответствующего законного основания.

8.4. ДОЛЖНА поддерживать требования о повторном рассмотрении, полученные через систему SSAD, и ДОЛЖНА рассматривать их, исходя из обоснования, представленного подателем запроса. Настоящим поясняется, что повторная подача запроса о раскрытии данных, идентичного исходному запросу, без обоснования необходимости повторного рассмотрения запроса, не требует повторного рассмотрения стороной, связанной договорными обязательствами.

8.5. При отсутствии каких-либо правовых требований об обратном, НЕЛЬЗЯ отказывать в раскрытии информации исключительно из-за отсутствия чего-либо из перечисленного ниже: (i) постановление суда; (ii) повестка с вызовом в суд; (iii) рассмотрение гражданского иска; (iv) процессуальные действия в рамках UDRP или URS; а также нельзя обосновать отказ в раскрытии данных исключительно тем фактом, что запрос основан только на предположительном нарушении прав на интеллектуальную собственность.

[22] См. также руководство по реализации № 17.

Требования к решению об авторизации

После получения запроса от диспетчера центрального шлюза сторона, связанная договорными обязательствами:

8.6. ДОЛЖНА провести проверку prima facie[23] допустимости запроса, то есть оценить, содержит ли запрос достаточно сведений для того, чтобы сторона, связанная договорными обязательствами, могла выполнить основательный обзор и обработать соответствующие базовые данные. Если сторона, связанная договорными обязательствами определяет, что такой запрос недопустим, например не содержит достаточных оснований для основательного обзора базовых данных, сторона, связанная договорными обязательствами, прежде чем отклонить запрос, ДОЛЖНА запросить у подателя запроса дополнительную информацию.

8.7. Если запрос признан допустимым на основании проверки prima facie, ДОЛЖНА провести основательный обзор запроса и базовых данных:

8.7.1. Если после оценки базовых данных сторона, связанная договорными обязательствами, примет обоснованное решение, что раскрытие запрошенных элементов данных не приведет к раскрытию персональных данных, сторона, связанная договорными обязательствами, ДОЛЖНА раскрыть данные, если такое раскрытие не запрещено в соответствии с применимым законодательством.[24] Настоящим поясняется: если выполнение запроса не приведет к раскрытию персональных данных, сторона, связанная договорными обязательствами, не обязана выполнять дальнейшую оценку запроса.

8.7.2. Если после оценки базовых данных сторона, связанная договорными обязательствами, определит, что раскрытие запрошенных элементов данных приведет к раскрытию персональных данных, сторона, связанная договорными обязательствами, ДОЛЖНА определить, как минимум, в рамках основательного обзора запроса и базовых данных:

8.7.2.1. есть ли у стороны, связанной договорными обязательствами, законные основания для раскрытия информации;[25]

[23] Согласно определению в Кембриджском словаре, на первый взгляд (исходя из того, что кажется правдой при первом рассмотрении или слушании).

[24] При рассмотрении вопроса о публикации закрытых данных юридических лиц, особенно в отношении НПО и сторон, занимающихся правозащитной деятельностью, которые могут быть защищены местным законодательством (например, законом о конституционных и уставных правах), сторона, связанная договорными обязательствами, должна учитывать влияние на отдельных людей, личность которых может быть идентифицирована при раскрытии данных юридического лица.

[25] См. также руководство по реализации № 17

8.7.2.2. все ли запрашиваемые элементы данных необходимы;[26]
8.7.2.3. требуется ли обеспечение баланса или проверка в соответствии с законным основанием, которое было определено стороной, связанной договорными обязательствами, согласно пункту 8.3.

8.8. Если для запроса необходима оценка баланса или проверка в соответствии с пунктом 8.7.2.3:
8.8.1. ДОЛЖНА раскрыть данные, если на основании своей оценки сторона, связанная договорными обязательствами, определит, что законный интерес подателя запроса не перевешивается интересами или основными правами и свободами субъекта данных. Сторона, связанная договорными обязательствами, ДОЛЖНА задокументировать обоснование своего разрешения.
8.8.2. ДОЛЖНА отклонить запрос, если на основании своей оценки сторона, связанная договорными обязательствами, определит, что законный интерес подателя запроса перевешивается интересами или основными правами и свободами субъекта данных. Сторона, связанная договорными обязательствами, ДОЛЖНА задокументировать обоснование своего отказа и ДОЛЖНА сообщить причину отказа диспетчеру центрального шлюза, при этом позаботившись о том, чтобы никакие персональные данные не были включены в причину отказа.

8.9. Если для запроса не нужна оценка баланса или проверка в соответствии с пунктом 8.7.2.3:
8.9.1. ДОЛЖНА раскрыть данные, если сторона, связанная договорными обязательствами, определит, что для этого имеется законное основание или это не запрещено действующим законодательством. Сторона, связанная договорными обязательствами, ДОЛЖНА задокументировать обоснование своего разрешения.
8.9.2. ДОЛЖНА отклонить запрос, если сторона, связанная договорными обязательствами, определит, что для раскрытия данных нет законных оснований или это запрещено в соответствии с действующим законодательством. Сторона, связанная договорными обязательствами, ДОЛЖНА задокументировать обоснование своего отказа и ДОЛЖНА сообщить причину отказа диспетчеру центрального шлюза, при этом позаботившись о том, чтобы никакие персональные данные не были включены в причину отказа.

[26] Дополнительную информацию об определении понятия «необходимый» см. на стр. 7 правовых рекомендаций, на которые опиралась Группа по EPDP при формулировании этого определения.

Податель запроса:

8.10. МОЖЕТ подать требование о повторном рассмотрении, если считает, что его запрос был отклонен незаконно.

8.11. ДОЛЖЕН в рамках своего требования о повторном рассмотрении представить обоснование необходимости повторного рассмотрения его запроса. Подтверждающее обоснование должно содержать достаточно подробную информацию о том, почему податель запроса считает, что его запрос был отклонен незаконно.

8.12. Если податель запроса считает, что сторона, связанная договорными обязательствами не соблюдает какие-либо требования настоящей политики, подателю запроса СЛЕДУЕТ уведомить корпорацию ICANN в дополнение к использованию механизма оповещения, описанного в рекомендации № 5 «Требования к ответам».

Руководство по реализации

8.13. Группа по EPDP предполагает, что сторона, связанная договорными обязательствами, сможет обмениваться сообщениями с подателем запроса посредством отдельной заявки в SSAD. Группа по EPDP также предполагает, что SSAD будет полностью защищена с помощью стандартной технологии защиты данных, включая шифрование для защиты передачи персональных данных в соответствии с действующим законодательством о защите данных и законами о кибербезопасности.

8.14. Группа по EPDP отмечает, что конкретные детали информационного обмена, указанного в пункте 8.6, будут определены на этапе реализации политики; тем не менее, Группа по EPDP предлагает в помощь это дополнительное руководство. Группа по EPDP предполагает, что сторона, связанная договорными обязательствами, отправит уведомление подателю запроса в рамках соответствующей заявки SSAD о своем решении отклонить запрос. У подателя запроса будет (x) дней для предоставления обновленной информации стороне, связанной договорными обязательствами. После предоставления подателем запроса обновленной информации срок ответа в рамках SLA обнуляется. Например, у стороны, связанной договорными обязательствами, будет 1 рабочий день для ответа на обновленный срочный запрос. Если податель запроса не предоставит информацию, выполнение SLA будет определяться временем отправки стороной, связанной договорными обязательствами, уведомления подателю запроса о своем намерении отказать. Если податель запроса не ответит, запрос будет отклонен по истечении установленного срока ответа.

8.15. В ситуациях, когда сторона, связанная договорными обязательствами, оценивает законный интерес подателя запроса, она ДОЛЖНА учитывать следующее:

8.15.1. Интерес должен быть конкретным, реальным и существующим, а не расплывчатым и спекулятивным.

8.15.2. Интерес обычно считается законным, если он проявлен в соответствии с законодательством о защите данных и другими законами.

8.15.3. Примеры законных интересов: (i) обеспечение исполнения, исполнение или защита законных требований, в том числе при нарушении прав на интеллектуальную собственность; (ii) предотвращение мошенничества и неправомерного использования услуг; (iii) физическая, ИТ и сетевая безопасность.

8.16. Стороне, связанной договорными обязательствами, СЛЕДУЕТ, в рамках своего основательного обзора, оценить, как минимум, следующее:

8.16.1. В соответствующих случаях следует использовать перечисленные ниже факторы, чтобы определить, что законный интерес подателя запроса не перевешивается интересами или основными правами и свободами субъекта данных. Ни один фактор не является определяющим; вместо этого сторона, связанная договорными обязательствами, ДОЛЖНА учитывать совокупность обстоятельств, изложенных ниже:

8.16.1.1. *Оценка воздействия*. Учитывайте прямое влияние на субъект данных, а также любые возможные более широкие последствия обработки данных. Учитывайте общественные интересы и законные интересы, преследуемые подателем запроса, например, для поддержания безопасности и стабильности DNS. Всякий раз, когда обстоятельства запроса о раскрытии или характер данных, которые должны быть раскрыты, предполагают повышенный риск для затронутого субъекта данных, это должно учитываться при принятии решений.

8.16.1.2. *Характер данных.* Учитывайте степень конфиденциальности данных, а также опубликованы ли они на данный момент.

8.16.1.3. *Статус субъекта данных.* Учитывайте, повышает ли статус субъекта данных его уязвимость (например, дети, претенденты на получение политического убежища, другие защищенные категории)

8.16.1.4. *Объем обработки.* Учитывайте сведения из запроса о раскрытии данных или другие соответствующие обстоятельства, которые указывают, будут ли данные надежно храниться (меньший риск) по сравнению с

публичным раскрытием, доступностью более широкой аудитории или объединением с другими данными (более высокий риск),[27] при условии, что это не направлено на запрет публичного раскрытия данных в рамках судебных или административных процедур разрешения споров, таких как UDRP или URS.

8.16.1.5. *Разумные ожидания субъекта данных.* Учитывайте, будет ли субъект данных ожидать на разумных основаниях обработки/раскрытия его данных таким способом.

8.16.1.6. *Статус контролера и субъекта данных.* Учитывайте переговорные возможности и любые диспропорции в полномочиях контролера и субъекта данных.[28]

8.16.1.7. *Задействованные правовые концепции.* Учитывайте нормативную базу юрисдикций подателя запроса, стороны, связанной договорными обязательствами, и субъекта данных, и то, как она может повлиять на потенциальное раскрытие данных.

8.16.1.8. *Трансграничная передача данных.* Учитывайте требования, которые могут быть применимы к трансграничной передаче данных.

8.17. Законное основание может опираться на наличие законного основания в рамках политики ICANN (или применимого права).

Применение проверки сбалансированности и факторов, рассматриваемых в этом разделе, СЛЕДУЕТ пересмотреть, в зависимости от ситуации, с учетом применимого прецедентного права, интерпретирующего GDPR, руководящих принципов, опубликованных EDPB, или изменений GDPR или других применимых законов о конфиденциальности, которые могут появиться в будущем.

Recommendation #9. Автоматизация обработки в SSAD

9.1. Группа по EPDP рекомендует ОБЯЗАТЬ диспетчера центрального шлюза автоматизировать получение, аутентификацию и передачу запросов SSAD соответствующей стороне, связанной договорными обязательствами, насколько это технически и коммерчески возможно и разрешено законом.

9.2. SSAD ДОЛЖНА давать возможность автоматизированной обработки правильно сформированных, действительных, полных, правильно

[27] Дополнительную информацию о повышении риска при объединении данных см. на стр. 5 правовых рекомендаций, на которые опиралась Группа по EPDP при рассмотрении этих факторов.

[28] В контексте авторизации стороны, связанной договорными обязательствами, соответствующими сторонами являются сторона, связанная договорными обязательствами, (контролер) и владелец домена (субъект данных); однако роли и обязанности сторон будут дополнительно обсуждаться в процессе реализации.

идентифицированных запросов со стороны аккредитованных пользователей, как описано ниже.

Автоматизированная обработка решений о раскрытии данных

9.3. Стороны, связанные договорными обязательствами, ДОЛЖНЫ обрабатывать решения о раскрытии данных в автоматизированном режиме по запросам любых категорий, для которых автоматизация (см. пункт 9.4 и процессы, описанные в рекомендации № 18) считается технически и коммерчески[29] осуществимой[30] и разрешенной законом. Во избежание разночтений настоящим поясняется, что Группа по EPDP рекомендует не исключать никакие категории решений о раскрытии данных, которые в настоящее время не соответствуют этим критериям, при рассмотрении в будущем возможности автоматического раскрытия данных в соответствии с процессами, подробно описанными в рекомендации № 18. В областях, где решения о раскрытии данных не отвечают этим критериям, основной целью является стандартизация процесса принятия решений о раскрытии данных.

9.4. Согласно полученным правовым рекомендациям (см. документ Консультация по примерам использования автоматизации в контексте раскрытия закрытых данных о владельцах доменов — апрель 2020 года), Группа по EPDP рекомендует ОБЯЗАТЕЛЬНО автоматизировать с момента запуска SSAD следующие типы запросов о раскрытии данных, для которых юридическая допустимость полной автоматизации (прием и обработка решения о раскрытии) зафиксирована в GDPR:

9.4.1. Запросы правоохранительных органов в местных или иным образом применимых юрисдикциях, когда 1) имеется подтвержденное законное основание согласно GDPR 6(1)e или 2) обработка должна выполняться в соответствии с исключением, указанным в статье 2 GDPR.

9.4.2. Расследование нарушения законодательства о защите данных, предположительно совершенного ICANN/стороной, связанной договорными обязательствами, и затрагивающего владельца домена.

[29] В ходе реализации потребуется дополнительно рассмотреть коммерческую осуществимость для регистраторов, которые могут получать весьма ограниченное количество запросов, отвечающих критериям автоматизированной обработки решений о раскрытии данных, и оценить, будет ли финансовое бремя применения автоматической обработки столь значительным, что придется сделать исключение. При рассмотрении этого вопроса диспетчер центрального шлюза также должен рассмотреть, как он может способствовать интеграции системы стороны, связанной договорными обязательствами, с SSAD, чтобы уменьшить любую потенциальную нагрузку от автоматизированной обработки решений о раскрытии данных.

[30] Первоначальный анализ финансовой осуществимости автоматизации будет выполнен корпорацией ICANN совместно с группой по анализу реализации, а затем с помощью механизма развития SSAD, если применимо.

9.4.3. Запрос только данных из поля «город» для оценки необходимости предъявить претензию или для статистических целей.
9.4.4. Отсутствие персональных данных в регистрационной записи, которая ранее была раскрыта стороной, связанной договорными обязательствами.

9.5. Настоящим поясняется: если сторона, связанная договорными обязательствами, определит, что автоматическая обработка решения о раскрытии данных для примеров использования, указанных в этой рекомендации, или при использовании процессов, описанных в рекомендации № 18, юридически недопустима или несет с собой значительный риск, который не был учтен в правовых рекомендациях, полученных Группой по EPDP, но впоследствии был выявлен и задокументирован, например, с помощью оценки влияния на защиту данных (DPIA), сторона, связанная договорными обязательствами, ДОЛЖНА уведомить корпорацию ICANN о том, что ей требуется освобождение от автоматизированной обработки решений о раскрытии данных для указанных примеров использования, и ДОЛЖНА приложить к уведомлению подтверждающую документацию. Необоснованные уведомления о необходимости освобождения МОГУТ быть рассмотрены корпорацией ICANN. Корпорация ICANN ДОЛЖНА аннулировать решение об освобождении, если обнаружит, что уведомление стороны, связанной договорными обязательствами, содержит недостоверную информацию или признаки злоупотребления.

9.6. Как только корпорация ICANN будет уведомлена, диспетчер центрального шлюза ДОЛЖЕН приостановить для указанных примеров использования передачу запросов, требующих автоматизированной обработки, и ДОЛЖЕН передать запрос в соответствии с требованиями рекомендации 8 «Авторизация сторон, связанных договорными обязательствами».

9.7. Корпорация ICANN ДОЛЖНА предусмотреть процесс приема уведомлений и комментариев, чтобы у затронутых заинтересованных сторон была возможность предоставить информацию о необходимости освобождения от выполнения требования, указанную в пункте 9.5. Корпорация ICANN МОЖЕТ способствовать последующим переговорам между затронутыми заинтересованными сторонами и соответствующей стороной, связанной договорными обязательствами, для содействия обоюдному пониманию исключительной ситуации и подтверждающей информации. Подробности, в том числе потенциальная конфиденциальность процесса, будут определены в процессе реализации.

9.8. Как только сторона, связанная договорными обязательствами, узнает, что исключение больше не применимо, она ДОЛЖНА проинформировать корпорацию ICANN соответствующим образом.

9.9. После получения уведомления от стороны, связанной договорными обязательствами, в соответствии с пунктом 9.8, диспетчер центрального шлюза ДОЛЖЕН передавать запросы, отвечающие критериям автоматизированной обработки, стороне, связанной договорными обязательствами, в соответствии с настоящей рекомендацией, а сторона, связанная договорными обязательствами, ДОЛЖНА возобновить автоматическую обработку решений о раскрытии данных для соответствующих примеров использования.

9.10. Что касается запросов о раскрытии данных, которые будут отправляться стороне, связанной договорными обязательствами, для проверки, сторона, связанная договорными обязательствами, МОЖЕТ предложить центральному шлюзу автоматизировать обработку решений о раскрытии данных для всех или некоторых видов запросов и (или) для запросов, поступающих от конкретного подателя запроса,[31] после того, как сторона, связанная договорными обязательствами, взвесит риск и оценит юридическую допустимость, если применимо.

9.11. Сторона, связанная договорными обязательствами, МОЖЕТ в любое время отозвать или пересмотреть запрос на автоматизацию решения о раскрытии данных, которое не требуется согласно этим рекомендациям по политике.

9.12. Настоящим поясняется, что диспетчер центрального шлюза следит за тем, отвечает ли запрос критериям автоматизированной обработки решений о раскрытии данных, что МОЖЕТ включать неавтоматизированную проверку на центральном шлюзе. По аналогии, центральный шлюз МОЖЕТ запросить у стороны, связанной договорными обязательствами, дополнительную информацию, которая поможет диспетчеру центрального шлюза определить, соблюдаются ли критерии автоматической обработки решений о раскрытии данных. Сторона, связанная договорными обязательствами, МОЖЕТ предоставить такую дополнительную информацию по запросу. Не ожидается, что в ответ на такой запрос информации будут переданы персональные данные.

[31] Например, сторона, связанная договорными обязательствами, может рассмотреть возможность внедрения схемы надежных уведомителей, которая позволит произвести квалификационный отбор подателей запросов, отвечающих определенным критериям, установленным соответствующей стороной, связанной договорными обязательствами, для автоматизированного ответа на их запросы о раскрытии данных.

Руководство по реализации

В дополнение к требованиям, изложенным в рекомендации № 4 (Подтверждение получения) и рекомендации № 10 (SLA), которые также будут применяться к автоматизированной обработке решений о раскрытии данных, следующее руководство по реализации распространяет свое действие на автоматическую обработку решений о раскрытии данных, то есть запросов, для которых диспетчер центрального шлюза определяет, что требуется автоматическое решение по запросу о раскрытии данных от стороны, связанной договорными обязательствами, в соответствии с этой рекомендацией.

9.13. Группа по EPDP ожидает, что такие аспекты SSAD, как прием запросов, проверка учетных данных, подтверждение отправки запроса (формат и полнота, а не содержание) можно автоматизировать, хотя, скорее всего, невозможно полностью автоматизировать все аспекты рассмотрения и выполнения запросов о раскрытии данных во всех случаях.

9.14. В контексте дальнейшего рассмотрения возможных примеров использования, которые считаются юридически допустимыми в контексте рекомендации № 18, юридическая допустимость будет определяться, в отсутствие авторитетных указаний (таких как указания EDPB и Европейского суда (ECJ) или новый закон), сторонами, отвечающими за автоматизированную обработку решений о раскрытии данных.

9.15. В дополнение к указанным выше правовым рекомендациям Группа по EPDP рекомендует Постоянному комитету GNSO (см. рекомендацию № 18) дополнительно рассмотреть оба механизма защиты, изложенные в Приложении 2 к документу Консультация по примерам использования автоматизации в контексте раскрытия закрытых данных о владельцах доменов — апрель 2020 года и в примерах использования, описанных в разделе 3.4 указанного консультативного документа, чтобы определить, будет ли раскрытие данных иметь юридический или аналогичный значительный эффект, который может помешать автоматизации.

9.16. Как ожидается, автоматизированная обработка решений о раскрытии данных будет работать на практике следующим образом: диспетчер центрального шлюза будет подтверждать, что запрос отвечает требованиям к автоматизированной обработке, и давать указание стороне, связанной договорными обязательствами, автоматически раскрыть запрашиваемые данные подателю запроса. Ожидается, что этот механизм будет определен в ходе реализации.

9.17. Все стороны, участвующие в SSAD, должны будут рассмотреть требования, которые могут применяться к трансграничной передаче данных.

Recommendation #10. Определение изменяемых SLA для сроков ответа в SSAD

10.1. Группа по EPDP рекомендует сторонам, связанным договорными обязательствами, ОБЯЗАТЕЛЬНО соблюдать соглашения об уровне обслуживания (SLA), которые разработаны, внедрены, имеют силу и периодически обновляются согласно рекомендации № 18 в соответствии с руководством по реализации, приведенным ниже.

10.2. В целях расчета срока ответа SLA Группа по EPDP рекомендует запускать отсчет SLA, когда подтвержденный запрос со всей вспомогательной информацией предоставлен стороне, связанной договорными обязательствами, диспетчером центрального шлюза, и останавливать, после того как сторона, связанная договорными обязательствами, (через центральный шлюз), предоставит запрашиваемые данные, ответит отказом или запросит дополнительную информацию. Запрос на повторное рассмотрение или ответ подателя запроса с дополнительной информацией будет считаться началом рассмотрения нового запроса для целей расчета SLA.

Таблица приоритетов для неавтоматизированных запросов о раскрытии данных

Тип запроса	Приоритет	Предлагаемое значение SLA[32] (соблюдение через 6 / 12 / 18 месяцев)
Срочные запросы	1	1 рабочий день, но не более 3 календарных дней (85% / 90% / 95%)
Административное производство ICANN	2	Не более 2 рабочих дней (85% / 90% / 95%)
Все остальные запросы*	3	См. руководство по реализации ниже.

*Примечание. Ничто в этих рекомендациях по политике не запрещает явным образом разработку новых категорий и определенных SLA.

Руководство по реализации

10.3. Требования приоритета 1 и 2 должны стать обязательными для исполнения в соответствии с документом согласованной политики. Требования к уровню обслуживания с приоритетом 3 также можно сделать обязательными для исполнения в составе документа согласованной политики после консультации с IRT.

[32] Обратите внимание, что указанные в таблице рабочие дни отсчитываются с момента получения стороной, связанной договорными обязательствами, запроса о раскрытии данных от диспетчера центрального шлюза.

Предлагаемые определения

Рабочие дни:[33] как определено в юрисдикции стороны, связанной договорными обязательствами.
Среднее время реагирования: скользящее среднее время по всем случаям реагирования, автоматически рассчитываемое (например, ежедневно или еженедельно) для помощи стороне, связанной договорными обязательствами, в оценке собственной эффективности в любой момент.
Интервал оценки целевого значения реагирования: трехмесячный период, позволяющий оценивать время реагирования 4 раза в год.
Целевое значение реагирования: величина среднего времени реагирования, измеренная в последний день интервала оценки целевого значения реагирования.
Целевое значение соблюдения договорных обязательств: то же определение, что и для целевого значения реагирования, но с проверкой соблюдения этого целевого SLA.

Требования к времени ответа стороны, связанной договорными обязательствами, на запросы SSAD будут повышаться в два этапа:

- Фаза 1 начинается через **6 (шесть) месяцев** после даты вступления в силу политики SSAD.
- Фаза 2 начинается через **1 (один) год** после даты вступления в силу политики SSAD.

ФАЗА 1 (применяется только к запросам с приоритетом 3)

10.4. Во время фазы 1 и в дальнейшем целевые показатели реагирования стороны, связанной договорными обязательствами, на запросы к SSAD с приоритетом 3 составляют 5 (пять) рабочих дней.

10.5. Диспетчер центрального шлюза ДОЛЖЕН измерять целевые показатели реагирования, используя среднее значение времени реагирования, а не отдельные ответы.

10.6. SSAD ДОЛЖНА рассчитывать среднее время реагирования стороны, связанной договорными обязательствами, как скользящее среднее, для помощи стороне, связанной договорными обязательствами, в оценке собственной эффективности в любой момент.

10.7. SSAD ДОЛЖНА также измерять целевое значение реагирования в виде текущего среднего значения в конце интервала оценки целевого значения

[33] См. также рекомендацию № 6.5.

реагирования. Для определения успеха или неудачи в достижении целей реагирования ДОЛЖНО использоваться только 3-месячное целевое значение реагирования, как описано ниже. Во избежание разночтений настоящим поясняется, что намерение сообщать в рамках SSAD стороне, связанной договорными обязательствами, среднее время реагирования нацелено на предупреждение стороны, связанной договорными обязательствами, о возможной проблеме со сроками ее реагирования и предоставление стороне, связанной договорными обязательствами, возможности устранить проблему в духе сотрудничества. Поэтому у сторон, связанных договорными обязательствами, всегда должен быть доступ для просмотра своего текущего целевого значения реагирования. Если целевое значение реагирования стороны, связанной договорными обязательствами, превышает 5 (пять) рабочих дней, это НЕ ДОЛЖНО считаться нарушением политики.

Вместо этого, если целевое значение реагирования не достигнуто, ICANN предупредит сторону, связанную договорными обязательствами, о несоблюдении целевого показателя реагирования.

10.8. Сторона, связанная договорными обязательствами, ДОЛЖНА ответить на уведомление ICANN о несоблюдении целевого показателя реагирования в течение 5 (пяти) рабочих дней.

10.9. Ответ стороны, связанной договорными обязательствами, должен включать причины того, почему сторона, связанная договорными обязательствами, не смогла обеспечить целевой срок реагирования.

10.10. Отсутствие ответа стороны, связанной договорными обязательствами, на уведомление ICANN ДОЛЖНО считаться нарушением политики; соответственно, отсутствие ответа на уведомление о несоблюдении обязательств приведет к запросу со стороны отдела по контролю исполнения договорных обязательств ICANN.

ФАЗА 2 (применяется только к запросам с приоритетом 3)

10.11. На фазе 2 целевые показатели стороны, связанной договорными обязательствами, по соблюдению договорных обязательств в сфере запросов SSAD с приоритетом 3 составляют 10 (десять) рабочих дней.

10.12. Диспетчер центрального шлюза ДОЛЖЕН измерять целевые показатели по соблюдению договорных обязательств, используя среднее значение времени реагирования, а не отдельные ответы. SSAD рассчитывает средний целевой показатель соблюдения обязательств стороной, связанной

договорными обязательствами, в последний день интервала оценки целевого показателя реагирования.

10.13. Если целевое значение реагирования стороны, связанной договорными обязательствами, превышает десять рабочих дней, это означает нарушение политики и, соответственно, к стороне, связанной договорными обязательствами, будут применены меры принуждения к соблюдению договорных обязательств.

10.14. Целевые показатели реагирования и соблюдения договорных обязательств ДОЛЖНЫ проверяться, как минимум, через каждые шесть месяцев в течение первого года, а затем ежегодно (в зависимости от результата первой проверки).

10.15. Целевые показатели реагирования на запросы о раскрытии данных, отвечающие критериям полной автоматизации ответов, получат дальнейшее развитие на этапе реализации, но ожидается, что они составят менее 60 секунд.

10.16. Группе по анализу реализации следует дополнительно рассмотреть влияние SLA в случаях, когда дополнительная информация запрашивается стороной, связанной договорными обязательствами, и предоставляется подателем запроса. (Для получения дополнительной информации см. рекомендацию № 8 «Авторизация сторон, связанных договорными обязательствами».)

Recommendation #11. Условия и положения SSAD

11.1. Группа по EPDP рекомендует, чтобы минимальные ожидания для соответствующих соглашений и политики, такие как условия использования SSAD, политика конфиденциальности SSAD, соглашение о раскрытии и политика допустимого использования, были дополнительно определены на этапе реализации, чтобы впоследствии они разработаны и внедрены организацией, ответственной за SSAD (корпорацией ICANN или третьей стороной, которой корпорация ICANN поручит взять на себя эту функцию контроля за соблюдением). Эти соглашения и политика ДОЛЖНЫ учитывать все рекомендации данной политики. Ожидается, что эти соглашения и политика будут разработаны и согласованы, в случае необходимости, сторонами, участвующими в SSAD, с учетом следующих рекомендаций по реализации.

11.2. Все необходимые соглашения, касающиеся обработки запросов данных через SSAD, ДОЛЖНЫ содержать положения, касающиеся трансграничной передачи данных, закрепляющие обязательство сторон, где это

применимо, обеспечить и предусмотреть надлежащий уровень защиты данных.

11.3. Условия и положения SSAD МОГУТ по мере необходимости обновляться корпорацией ICANN с учетом применимого законодательства и практики.

Руководство по реализации:

11.4. Политика конфиденциальности SSAD в сфере обработки персональных данных пользователей SSAD (подателей запросов в SSAD и сторон, связанных договорными обязательствами)

Группа по EPDP рекомендует, как минимум, ОБЯЗАТЕЛЬНО включить в состав политики конфиденциальности соответствующие принципы защиты данных, в том числе:

- Вид (виды) обрабатываемых персональных данных
- Порядок и причины обработки персональных данных, например
    - проверка личности
    - передача служебных уведомлений
- Срок хранения персональных данных
- Категории третьих лиц, которым передаются персональные данные
- Где применимо, сведения о любой международной передаче данных / требования к такой передаче
- Информация о правах субъектов данных и способах реализации ими этих прав
- Уведомление о том, как будет происходить информирование об изменениях в политике конфиденциальности
- Требования к транспарентности
- Требования к безопасности данных
- Меры по обеспечению подотчетности (принцип «privacy by design», по умолчанию, сотрудник по защите данных (DPO) при превышении определенного объема и т. д.)

11.5. Условия использования для пользователей SSAD (подателей запросов в SSAD и сторон, связанных договорными обязательствами)

EPDP рекомендует, как минимум, ОБЯЗАТЕЛЬНО включить в условия использования следующее:

- Освобождение контролеров (организации, ответственной за принятие решения о раскрытии данных) от ответственности подателем запроса на основе следующих принципов:
    - Податели запросов несут ответственность за убытки или расходы, связанные с претензиями третьих сторон,

возникающими в результате (i) предоставления ими ложных сведений в процессе аккредитации или запроса; или (ii) неправомерного использования запрошенных данных в нарушение применимых условий использования или законов.
    - Ничто в настоящих условиях не ограничивает ответственность или права сторон на взыскание ущерба в соответствии с применимым законодательством (то есть подателям запросов не запрещается требовать возмещения от контролеров, если такие права предусмотрены законом).
    - Ничто в настоящих условиях не должно толковаться как введение обязательства по защите от ответственности для подателей запросов из государственных органов, у которых нет юридических полномочий для подписания таких оговорок о защите от ответственности. Кроме того, ничто в этом пункте не должно изменять потенциально существующую ответственность государства, которая служит средством правовой защиты операторов SSAD.
- Требования к запросам данных
- Требования к ведению журналов и аудиту
- Возможность продемонстрировать соответствие требованиям
- Применимые запреты
- Требования по предотвращению злоупотреблений

11.6. Соглашения о раскрытии данных для подателей запросов в SSAD

EPDP рекомендует, как минимум, ОБЯЗАТЕЛЬНО включить в соглашения о раскрытии данных требования к подателям запросов, вступающие в силу после раскрытия данных:

- Использование данных для цели, указанной в запросе
- Требования к использованию данных для иной цели, отличной от указанной в запросе
- Хранение и уничтожение данных: Податели запросов ДОЛЖНЫ подтвердить, что они будут хранить, защищать и удалять регистрационные данные gTLD в соответствии с действующим законодательством. Податели запросов ДОЛЖНЫ хранить регистрационные данные gTLD только до тех пор, пока это необходимо для достижения цели, указанной в запросе о раскрытии данных, если не требуется хранить такие данные в течение более длительного срока в соответствии с применимым законодательством.
- Законное использование данных

11.7. Политика допустимого использования для подателей запросов к SSAD. Податель запроса ДОЛЖЕН принять Политику допустимого использования перед отправкой запросов о раскрытии данных через SSAD.

Как минимум, Политика допустимого использования ДОЛЖНА содержать следующие требования:

Податель запроса:

11.7.1. ДОЛЖЕН запрашивать данные только из текущего набора данных RDS (без исторических данных).
11.7.2. ДОЛЖЕН для каждого запроса данных RDS предоставлять информацию о соответствующей цели и законном основании для обработки, которая будет подлежать аудиту (для получения дополнительной информации см. рекомендацию по аудиту № 16).
11.7.3. МОЖЕТ запрашивать данные из SSAD для нескольких целей в каждом запросе для одного и того же запрошенного набора данных.
11.7.4. Для каждой заявленной цели необходимо предоставить (i) информацию о предполагаемом использовании запрошенных данных и (ii) заверение в том, что податель запроса будет обрабатывать данные только для заявленных целей. Эти заверения подлежат аудиту (см. дополнительную информацию в рекомендации №16 по аудиту).

Recommendation #12. Требование к раскрытию данных

12.1. Группа по EPDP рекомендует следующее:

Стороны, связанные договорными обязательствами:

12.1.1. ДОЛЖНЫ раскрывать только данные, запрошенные подателем запроса.
12.1.2. ДОЛЖНЫ возвращать текущие данные или их подмножество (без исторических данных).

12.2. Стороны, связанные договорными обязательствами, и диспетчер центрального шлюза:

12.2.1. ДОЛЖНЫ обрабатывать данные в соответствии с действующим законодательством.
12.2.2. В случаях, предусмотренных применимым законодательством, ДОЛЖНЫ раскрыть владельцу зарегистрированного имени (субъекту данных), по обоснованному запросу, подтверждение обработки относящихся к нему персональных данных, однако с учетом того, что характер юридических расследований или процедур МОЖЕТ потребовать от SSAD и (или) раскрывающей

данные организации сохранять в тайне от субъекта данных характер или наличие определенных запросов. Конфиденциальные запросы МОГУТ быть раскрыты субъектам данных в сотрудничестве с подателем запроса и в соответствии с правами субъекта данных в рамках применимого законодательства.

12.2.3. В случаях, когда этого требует действующее законодательство, ДОЛЖНЫ предоставить механизм, с помощью которого субъект данных может реализовать свое право на удаление, возражать против автоматизированной обработки своей персональной информации, если такая обработка имеет юридические или аналогичные существенные последствия, а также реализовать любые другие применимые права.

12.2.4. ДОЛЖНЫ в краткой, транспарентной, понятной и легкодоступной форме, используя ясный и простой язык, уведомлять субъектов данных о типах организаций/третьих лиц, которые могут обрабатывать их данные. Во избежание разночтений настоящим поясняется, что стороны, связанные договорными обязательствами, ДОЛЖНЫ предоставить вышеописанное уведомление своим клиентам-владельцам доменов, а SSAD ДОЛЖНА предоставить вышеописанное уведомление пользователям SSAD. Для сторон, связанных договорными обязательствами, это уведомление ДОЛЖНО содержать информацию о потенциальных получателях закрытых регистрационных данных, включая, помимо прочего, получателей, перечисленных в рекомендации № 7 «Цели подателя запроса», в допустимых законом пределах. Дополнительно могут применяться информационные обязанности в соответствии с действующим законодательством, но информация, указанная выше, ДОЛЖНА содержаться в любом случае.

Руководство по реализации

12.3. Текущие данные означают данные, проверенные стороной, связанной договорными обязательствами, при вынесении решения о раскрытии данных. Чтобы снизить вероятность изменения данных во время рассмотрения запроса о раскрытии, например если владелец домена обновляет свои контактные данные, сторонам, связанным договорными обязательствами, рекомендуется раскрывать данные как можно скорее после принятия решения о раскрытии. Во избежание разночтений настоящим поясняется, что исторические данные представляют собой регистрационные данные, имевшиеся до подачи запроса о раскрытии, а не регистрационные данные, которые могли измениться в результате любых обновлений, сделанных владельцем домена с момента рассмотрения запроса о раскрытии и до решения о разглашении регистрационных данных.

12.4. Характер юридических расследований или процедур не ограничивается уголовными расследованиями или другими расследованиями (например, многие гражданские расследования требуют конфиденциальности).

Recommendation #13. Политика запросов

13.1. В отношении диспетчера центрального шлюза Группа по EPDP рекомендует следующее:

13.1.1. ДОЛЖЕН контролировать систему и предпринимать соответствующие действия,[34] такие как отмена или ограничение доступа для защиты от злоупотреблений или неправильного использования системы.

13.1.2. МОЖЕТ принимать меры по ограничению количества запросов, отправляемых одним подателем запроса, если будет продемонстрировано, что запросы имеют признаки злоупотребления.

К «злоупотреблениям» при использовании SSAD МОЖНО отнести (среди прочего) один или несколько из следующих типов поведения/действий:

13.1.2.1. Автоматическая отправка большого количества искаженных или неполных запросов.

13.1.2.2. Большое количество[35] автоматических дублирующихся запросов следующего характера: необоснованные, злонамеренные или сутяжнические.

13.1.2.3. Использование ложных, украденных или поддельных учетных данных для доступа к системе.

13.1.2.4. Хранение/задержка и отправка большого количества запросов, становящиеся причиной несоблюдения SLA у SSAD или других сторон. При расследовании злоупотреблений на основе этого конкретного поведения, следует учитывать понятие соразмерности.

13.1.3. Как и в случае других нарушений политики доступа, поведение с признаками злоупотребления может в конечном итоге привести к приостановке или прекращению доступа к SSAD. Если диспетчер центрального шлюза принимает решение ограничить количество запросов от подателя запроса из-за злоупотреблений, податель

[34] Группа по EPDP ожидает, что «соответствующие действия» будут дополнительно определены на этапе реализации.

[35] Группа по EPDP ожидает, что термин «большое количество» будет дополнительно определен на этапе реализации.

запроса МОЖЕТ требовать возмещения ущерба[36] через корпорацию ICANN, если сочтет такое решение необоснованным. Во избежание разночтений настоящим поясняется, что получение в SSAD большого количества запросов от одного и того же подателя запроса само по себе не должно приводить к фактическому вынесению решения о злоупотреблении системой.

13.1.4. ДОЛЖЕН отвечать только на запросы по конкретному доменному имени, для которого запрашиваются закрытые регистрационные данные, и ДОЛЖЕН изучать[37] каждый запрос индивидуально, а не массово, независимо от того, выполняется ли рассмотрение автоматически или путем полноценной проверки.

13.2. В отношении сторон, связанных договорными обязательствами, Группа по EPDP рекомендует следующее:

13.2.1. НЕ ДОЛЖНЫ отклонять запросы о раскрытии данных от SSAD на основании поведения с признаками злоупотребления, которое не было признано таковым диспетчером центрального шлюза в соответствии с пунктами a) и b) выше. Однако стороны, связанные договорными обязательствами, также должны иметь средства, позволяющие сообщить о таком поведении CGM/SSAD. Диспетчер центрального шлюза ДОЛЖЕН предоставить сторонам, связанным договорными обязательствами, механизм для сообщений о признаках злоупотреблений со стороны подателей запросов и в запросах и вынести решение относительно такого подателя запроса/запроса в сроки, позволяющие стороне, связанной договорными обязательствами, представить ответ. В качестве альтернативы стороне, связанной договорными обязательствами, будет разрешено отложить представление ответа до тех пор, пока диспетчер центрального шлюза не рассмотрит сообщение о злоупотреблении и не вынесет решение.

13.3. Группа по EPDP рекомендует следующее:

13.3.1. Диспетчер центрального шлюза ДОЛЖЕН поддерживать запросы по полностью определенным доменным именам (без символов обобщения имени).

[36] Настоящим поясняется, что возмещение ущерба будет иметь вид повторного рассмотрения запроса диспетчером центрального шлюза, для чего податель запроса может представить новую информацию, но не обязан это делать.

[37] Ожидается, что это изучение будет выполняться автоматически.

13.3.2. Диспетчер центрального шлюза ДОЛЖЕН предоставить подателю запроса возможность отправлять несколько доменных имен в одном запросе.[38]

13.3.3. Для запросов о раскрытии данных, не подлежащих автоматизированной обработке решения о раскрытии, диспетчер центрального шлюза ДОЛЖЕН направлять информацию по каждому домену индивидуально стороне, связанной договорными обязательствами, ответственной за решение о раскрытии (для этого может потребоваться, чтобы SSAD разделяла запрос на несколько транзакций).

13.3.4. Безотносительно к рекомендациям, касающимся борьбы со злоупотреблениями, диспетчер центрального шлюза и стороны, связанные договорными обязательствами, ДОЛЖНЫ иметь возможность обработки разумного количества запросов в соответствии с установленными SLA.

13.3.5. Диспетчер центрального шлюза ДОЛЖЕН поддерживать только запросы о раскрытии текущих данных (не касающиеся исторических регистрационных данных доменного имени).

13.3.6. SSAD ДОЛЖНА иметь возможность сохранять историю различных запросов о раскрытии данных, чтобы отслеживать переписку через SSAD между подателями запросов в SSAD и сторонами, связанными договорными обязательствами. Необходимо принять надлежащие меры для защиты этой информации. Соответствующий доступ к таким актуальным статистическим данным должен предоставляться СР, если это необходимо, чтобы обеспечить доступность всей важной информации, относящейся к запросам о раскрытии данных, для рассмотрения при принятии таких решений о раскрытии данных.

См. также требования политики допустимого использования в рекомендации № 11 «Условия и положения».

Руководство по реализации

13.4. Поведение с признаками злоупотребления может в конечном итоге привести к приостановке или прекращению доступа к SSAD; тем не менее, на этапе реализации следует рассмотреть схему ступенчатых штрафных санкций. Однако могут быть определенные случаи вопиющего злоупотребления, такие как фальсификация или кража учетных данных, когда доступ будет прекращен немедленно.

[38] Группа по EPDP ожидает, что на этапе реализации будет определено, сколько запросов может быть отправлено за раз, в соответствии с политикой запросов.

13.5. Запрос SSAD должен быть получен для каждой регистрации доменного имени, для которой требуется разглашение закрытых данных, но податели запросов должны иметь возможность одновременной отправки нескольких запросов, например путем ввода нескольких зарегистрированных доменных имен в той же форме запроса, при условии, что информация запроса не меняется.

13.6. Что касается положения «Соответствующий доступ к таким актуальным статистическим данным должен предоставляться CP, если это необходимо» в пункте 13.3, ожидается, что это будет ограничиваться собственной деятельностью CP.

Recommendation #14. Финансовая устойчивость

14.1. Группа по EPDP рекомендует при рассмотрении затрат и финансовой устойчивости SSAD разграничить разработку и ввод в действие системы и последующую эксплуатацию системы.

14.2. Цель состоит в том, чтобы SSAD была финансово самодостаточной и не становилась причиной каких-либо дополнительных сборов с владельцев доменов. Субъекты данных НЕ ДОЛЖНЫ нести расходы по раскрытию данных третьим сторонам; расходы на поддержание этой системы в первую очередь должны нести податели запросов в SSAD. Кроме того, субъекты данных НЕ ДОЛЖНЫ нести расходы по обработке запросов о раскрытии данных, которые были отклонены сторонами, связанными договорными обязательствами, после оценки запросов, отправленных пользователями SSAD. ICANN МОЖЕТ внести свой вклад в (частичное) покрытие расходов на содержание центрального шлюза. Настоящим поясняется: Группа по EPDP понимает, что владельцы доменов в конечном итоге являются источником большей части доходов ICANN. Этот доход сам по себе не нарушает ограничение, что «[c]убъекты данных НЕ ДОЛЖНЫ нести расходы по раскрытию данных третьим сторонам». Центральному шлюзу ЗАПРЕЩАЕТСЯ взимать отдельную плату с субъектов данных за запрос или раскрытие их данных третьим сторонам. Однако Группа по EPDP отмечает, что владельцы зарегистрированных имен всегда оплачивают любые расходы, понесенные регистраторами и регистратурами. Группа по EPDP также понимает, что RAA запрещает ICANN ограничивать размер платы, которую могут взимать регистраторы. Пункт 3.7.12 RAA гласит: «Никакими из положений настоящего соглашения не предписывается и не ограничивается сумма сборов, которые регистратор может взимать с владельцев зарегистрированных имен за регистрацию таких имен».

14.3. С потенциальными пользователями SSAD, определенными на этапе реализации процесса аккредитации, и провайдерами идентификации,

которые будут использоваться, следует проконсультироваться по вопросу определения размера сборов за использование SSAD. В частности, потенциальные податели запросов в SSAD, не являющиеся членами сообщества ICANN, должны иметь возможность отправлять комментарии и взаимодействовать с IRT. Этот вклад должен помочь в сборе информации для обсуждения этой темы в IRT.

14.4. SSAD НЕ СЛЕДУЕТ рассматривать как платформу для получения прибыли корпорацией ICANN или сторонами, связанными договорными обязательствами. Финансирование SSAD должно быть достаточным для покрытия расходов, в том числе на субподрядчиков, по справедливой рыночной стоимости и для создания фонда юридических рисков.[39] Очень важно обеспечить, чтобы любые платежи в SSAD были связаны с эксплуатационными расходами, а не являлись просто обменом денег на закрытые регистрационные данные.

14.5. В отношении концепции аккредитации:

14.5.1. С подателей заявок на аккредитацию ДОЛЖЕН взиматься подлежащий определению невозмещаемый сбор, пропорциональный стоимости проверки заявки; в определенных обстоятельствах эти сборы могут быть отменены или сделаны нулевыми для конкретных типов или категорий заявителей, которые СЛЕДУЕТ дополнительно определить на этапе реализации.

14.5.2. Заявители, получившие отказ, МОГУТ подать повторную заявку, но за рассмотрение новой заявки также МОЖЕТ взиматься сбор.

14.5.3. Сборы устанавливаются органом по аккредитации. Если орган по аккредитации передаст на аутсорсинг функцию провайдера идентификации, последний МОЖЕТ установить свои собственные сборы после консультации с органом по аккредитации.

14.5.4. Аккредитованные пользователи и организации ДОЛЖНЫ периодически продлевать свою аккредитацию.

Руководство по реализации

14.6. Группа по EPDP ожидает, что затраты на разработку, развертывание и ввод в действие этой системы, как и в случае реализации других принятых рекомендаций по политике, изначально несут корпорация ICANN,[40]

[39] Учитывая потенциальную правовую неопределенность и повышенный правовой и операционный риск для всех сторон, обеспечивающих работу SSAD, создание фонда юридических рисков подразумевает создание подходящего плана действий в чрезвычайных ситуациях правового характера, включая, помимо прочего, соответствующее страховое покрытие и любые другие надлежащие меры, которые могут быть сочтены достаточными для покрытия потенциальных штрафов регулирующих органов или соответствующих судебных издержек.

[40] См. также комментарий, который корпорация ICANN представила по запросу Группы по EPDP в отношении сметы расходов на предлагаемую систему стандартизованного доступа к закрытым регистрационным данным и их раскрытия (см. https://community.icann.org/x/GIIEC)

стороны, связанные договорными обязательствами и другие стороны, которые могут быть вовлечены.[41] В рамках ввода в действие SSAD корпорация ICANN, как ожидается, в целях снижения затрат рассмотрит возможность использования существующих механизмов или процесса RFP, вместо того, чтобы создавать SSAD и ее компоненты с нуля. Группа по EPDP ожидает, что SSAD в конечном итоге приведет к равным или меньшим затратам для сторон, связанных договорными обязательствами, по сравнению с получением и рассмотрением запросов вручную, что можно считать критерием коммерческой и технической осуществимости.

14.7. Ожидается, что дальнейшая эксплуатация системы будет происходить на основе возмещения затрат, при этом могут учитываться исторические затраты.[42] Например, расходы, связанные с получением аккредитации, будут нести стороны, запрашивающие аккредитацию. Точно так же некоторые затраты на функционирование SSAD СЛЕДУЕТ компенсировать за счет взимания платы с пользователей SSAD.

14.8. При внедрении и эксплуатации SSAD следует избегать непропорционально высокой нагрузки на небольших операторов.

14.9. Группа по EPDP признает, что сборы, связанные с использованием SSAD, могут различаться для пользователей в зависимости от объема запросов или типа пользователя, наряду с другими потенциальными факторами. Группа по EPDP также признает, что для государственных органов могут существовать определенные платежные ограничения, которые следует учитывать на этапе реализации.

14.10. Структура сборов, а также период продления должны быть определены на этапе реализации в соответствии с изложенными выше принципами. Группа по EPDP признает, что возможность установить точный размер сборов может появиться только тогда, когда станут известны фактические затраты. Группа по EPDP также признает, что структура сборов SSAD с течением времени может пересматриваться.

Recommendation #15. Ведение журналов

15.1. Группа по EPDP рекомендует ОБЯЗАТЕЛЬНО ввести в действие соответствующие процедуры ведения журналов для облегчения процедур аудита, описанных в этих рекомендациях. Эти требования к регистрации будут охватывать следующее:

[41] Настоящим поясняется, что корпорация ICANN будет нести свои собственные расходы по разработке системы. Стороны, связанные договорными обязательствами, будут нести самостоятельную ответственность за собственные расходы.

[42] Исторические затраты — это затраты на разработку, развертывание и ввод в действие системы.

- Орган по аккредитации
- Диспетчер центрального шлюза
- Провайдер идентификации
- Стороны, связанные договорными обязательствами
- Действия аккредитованных пользователей, например попытки входа в систему, запросы
- Отправленные запросы и принятые решения о раскрытии данных

15.2. Группа по EPDP рекомендует следующее:

15.2.1. Диспетчер центрального шлюза ДОЛЖЕН вести журналы всех действий всех субъектов, которые взаимодействуют с диспетчером центрального шлюза (дополнительные сведения см. ниже).

15.2.2. В журналах ДОЛЖНЫ быть зарегистрированы все запросы и сведения, необходимые для аудита любых решений, принятых в контексте SSAD.

15.2.3. Журналы ДОЛЖНЫ храниться в течение срока, достаточного для целей аудита и рассмотрения жалоб, с учетом установленных законом ограничений в отношении жалоб на контролера.

15.2.4. Журналы НЕ ДОЛЖНЫ содержать никакой персональной информации. Если регистрируется какая-либо информация, которая действительно содержит персональные данные, должны быть приняты соответствующие меры безопасности. Журналы МОГУТ использоваться для подготовки отчетов о транспарентности, которые могут быть общедоступными. (См. также рекомендацию № 17 по требованиям к отчетности.) Зарегистрированные данные, содержащие персональную информацию, ДОЛЖНЫ оставаться конфиденциальными.

15.2.5. Журналы ДОЛЖНЫ храниться в общепринятом,[43] пригодном для машинного считывания формате с понятным описанием всех переменных.

15.2.6. Соответствующие зарегистрированные данные ДОЛЖНЫ раскрываться, когда это разрешено законом, в следующих обстоятельствах:

- В случае заявления о неправильном использовании журналы могут быть запрошены для изучения органом по аккредитации или поставщиком услуг по разрешению споров.
- Журналы должны быть также доступны ICANN и аудиторскому органу.
- Когда это необходимо сделать в результате надлежащей правовой процедуры, включая процедуры соответствующих правоохранительных и регулирующих органов, если применимо.

[43] Настоящим поясняется, что «общепринятый» — это формат, который используется многими, в отличие от единого формата для всех.

15.2.7. Соответствующие зарегистрированные данные МОГУТ быть раскрыты для следующих целей:
- Общая техническая эксплуатация для обеспечения правильной работы системы.

15.2.8. Соответствующие журналы следует использовать в качестве источника любых уместных данных. Эти данные должны позволять подателям запросов и сторонам, связанным договорными обязательствами, просматривать свою собственную статистику.

15.3. Как минимум, ДОЛЖНЫ регистрироваться следующие события:
- Ведение журналов применительно к провайдеру идентификации[44]
- Ведение журналов применительно к органу по аккредитации
  - Подробная информация о поступающих запросах на аккредитацию
  - Результаты обработки запросов на аккредитацию, например, выдача удостоверений личности или причины отказа
  - Подробная информация о запросах на отзыв
  - Индикация завершения проверки подлинности удостоверений личности и подписанных утверждений.
  - Уникальный ссылочный номер
- Ведение журналов применительно к диспетчеру центрального шлюза
  - Информация о содержании самого запроса.
  - Результаты обработки запроса, включая изменения состояния (например, получено, ожидает рассмотрения, обрабатывается, отклонено, одобрено, одобрено с изменениями)
  - Показатели:
    - раскрытие и неразглашение;
    - использование каждой причины отказа в случае неразглашения;
    - расхождение между решениями CP о раскрытии и неразглашении и рекомендациями центрального шлюза.

Ведение журналов, относящихся к сторонам, связанным договорными обязательствами
- Подробные сведения об ответе на запрос, например, причина отказа, уведомление об одобрении и опубликованные поля данных. Необходимо хранить решения о раскрытии данных, включая причину отказа.

Recommendation #16. Аудиторские проверки

16.1. Группа по EPDP рекомендует ОБЯЗАТЕЛЬНО внедрить соответствующие процессы и процедуры аудита для обеспечения надлежащего мониторинга и соблюдения требований, изложенных в данных рекомендациях.

[44] Должно быть подробнее описано на этапе реализации.

16.2. При проведении любой проверки аудитор ДОЛЖЕН соблюдать разумные обязательства по сохранению конфиденциальности в рамках собственных процессов и в отношении персональной информации, раскрываемой в ходе аудита.

Конкретнее:

Аудиторские проверки органа по аккредитации

16.3. Если ICANN передает функцию органа по аккредитации на аутсорсинг квалифицированной третьей стороне, орган по аккредитации ДОЛЖЕН периодически проходить проверку для обеспечения соблюдения требований политики, как определено в рекомендации по аккредитации. Если будет обнаружено, что орган по аккредитации нарушает политику и требования к аккредитации, ему будет предоставлена возможность исправить нарушение, но в случае повторного нарушения или отрицательного результата аудита необходимо выбрать или создать новый орган по аккредитации. Корпорация ICANN как орган по аккредитации не обязана проводить аудит государственных организаций, чьи требования к аккредитации и аудиту определены в рекомендации № 2.

16.4. Аудит органа по аккредитации ДОЛЖЕН быть направлен именно на оценку выполнения условий соглашения, и аудитор ДОЛЖЕН заблаговременно (по разумному усмотрению) отправить уведомление о любой такой проверке, в котором будет в разумной степени подробно указано, какие категории документов, данные и другая информация потребуются.

16.5. В рамках таких аудиторских проверок орган по аккредитации ДОЛЖЕН своевременно предоставить аудитору все необходимые документы, данные и любую другую информацию, необходимую для демонстрации соблюдения политики аккредитации.

16.6. Если ICANN выступает в качестве органа по аккредитации, ожидается, что существующие механизмы подотчетности устранят любые нарушения политики аккредитации, с учетом того, что в таком крайнем случае учетные данные, выданные во время нарушения, будут проверены. Процедуры такой проверки СЛЕДУЕТ создать на этапе реализации.

Аудит провайдеров идентификации

16.7. Провайдеры идентификации ДОЛЖНЫ периодически проходить проверку для обеспечения соблюдения требований политики, как определено в рекомендации по аккредитации. Если будет обнаружено, что провайдер

идентификации нарушает политику и требования к аккредитации, ему будет предоставлена возможность исправить нарушение, но в случае повторного нарушения или отрицательного результата аудита необходимо выбрать нового провайдера идентификации.

16.8. Аудит провайдера идентификации ДОЛЖЕН быть направлен именно на оценку выполнения условий соглашения, и аудитор ДОЛЖЕН заблаговременно (по разумному усмотрению) отправить уведомление о любой такой проверке, в котором будет в разумной степени подробно указано, какие категории документов, данные и другая информация потребуются.

16.9. В рамках таких аудиторских проверок провайдер идентификации ДОЛЖЕН своевременно предоставить аудитору все необходимые документы, данные и любую другую информацию, необходимую для демонстрации соблюдения политики аккредитации.

Аудит аккредитованных юридических и физических лиц

16.10. Соответствующие механизмы ДОЛЖНЫ быть разработаны на этапе реализации, чтобы гарантировать соответствие аккредитованных организаций и физических лиц требованиям политики, как определено в рекомендациях по аккредитации № 1 и 2. Например, к ним могут относиться аудиторские проверки, инициированные подтвержденными жалобами, выборочные аудиторские проверки или проверки в ответ на самосертификацию или самооценку. Если будет обнаружено, что аккредитованная организация или физическое лицо нарушает политику и требования к аккредитации, ему будет предоставлена возможность исправить нарушение, но в случае повторного нарушения или отрицательного результата аудита дело следует вернуть в орган по аккредитации и (или) провайдеру идентификации, если применимо, для принятия мер.

16.11. Аудит аккредитованных организаций или физических лиц ДОЛЖЕН быть направлен именно на оценку выполнения условий соглашения, и аудитор ДОЛЖЕН заблаговременно (по разумному усмотрению) отправить уведомление о любой такой проверке, в котором ДОЛЖНО быть в разумной степени подробно указано, какие категории документов, данные и другая информация потребуются.

16.12. В рамках таких аудиторских проверок аккредитованное юридическое или физическое лицо ДОЛЖНО своевременно предоставить аудитору все необходимые документы, данные и любую другую информацию, необходимую для демонстрации соблюдения политики аккредитации.

Recommendation #17. Требования к отчетности

17.1. Группа по EPDP рекомендует ОБЯЗАТЬ корпорацию ICANN составлять регулярные публичные отчеты об использовании и функционировании SSAD. Во избежание разночтений настоящим поясняется, что эта рекомендация не препятствует подготовке корпорацией ICANN дополнительных конфиденциальных отчетов для пользователей SSAD.

17.2. Не ранее, чем через 3 месяца и не позднее, чем через 9 месяцев после ввода в действие SSAD, корпорация ICANN ДОЛЖНА опубликовать отчет о состоянии дел в SSAD или панель управления, и делать это в дальнейшем ежеквартально. При этом должна быть представлена, как минимум, следующая информация:

- количество полученных запросов о раскрытии данных;
- среднее время ответа на запросы о раскрытии данных с разбивкой по уровню приоритета;
- количество запросов, классифицированных по целям/обоснованиям третьих сторон (как указано в рекомендации № 4);
- количество одобренных и отклоненных запросов о раскрытии;
- количество запросов о раскрытии данных, обработанных в автоматическом режиме;
- количество запросов, обработанных вручную;
- информация о финансовой устойчивости SSAD;
- новые руководящие указания EDPB или новая актуальная правовая практика (если имеется);
- технические или системные трудности;
- эксплуатационные и системные улучшения.

Руководство по реализации:

17.3. Группа по EPDP рекомендует во время реализации уделить дополнительное внимание следующему:

- Периодичность публичных отчетов — публичная отчетность на ежеквартальной основе представляется целесообразной.
- Данные, подлежащие отражению в отчетах, которые, как ожидается, будут включать такую информацию, как: а) количество запросов о раскрытии; б) запросы о раскрытии данных по категориям запрашивающих; в) запросы о раскрытии данных по подателям запросов (для юридических лиц); удовлетворенные/отклоненные запросы о раскрытии данных; время реагирования. Обратите внимание, что это неполный список.

- Механизм публичной отчетности — следует рассмотреть возможность создания общедоступной панели управления вместо публикуемых отчетов или в дополнение к ним.
- Потребности в возможной конфиденциальности в определенных случаях, например, информация о физических лицах и запросы LEA. Для решения возможных проблем конфиденциальности можно рассмотреть агрегирование или псевдонимизацию данных.

Recommendation #18. Анализ реализации рекомендаций по политике в отношении SSAD с помощью Постоянного комитета GNSO

18.1. Группа по EPDP рекомендует Совету GNSO ОБЯЗАТЕЛЬНО создать Постоянный комитет GNSO для оценки операционных проблем SSAD, возникающих в результате принятия и (или) реализации согласованной политики ICANN. Постоянный комитет GNSO предназначен для изучения данных, получаемых в результате работы SSAD, и предоставления Совету GNSO рекомендаций о наиболее полезных операционных изменениях в SSAD, которые являются исключительно мерами по реализации, в дополнение к рекомендациям, основанным на анализе влияния действующей согласованной политики в отношении работы SSAD.

18.2. Группа по EPDP также рекомендует Совету GNSO использовать следующие принципы в качестве основы для выполнения Постоянным комитетом GNSO своей миссии, которая должна быть отражена в его уставе:

18.2.1 Состав: В состав Постоянного комитета GNSO входят консультативные комитеты ICANN, а также группы заинтересованных сторон и группы интересов GNSO, представленные в текущей Группе по EPDP в области Временной спецификации для регистрационных данных в gTLD. В его состав должен входить, как минимум, один член из GAC, ALAC, SSAC, RySG, RrSG, NCSG, IPC, BC и ISPCP, а также, как минимум, один дублер от каждой группы. Обратите внимание, что количество членов в группе не должно повлиять на процесс достижения консенсуса, поскольку предполагается, что позиции будут рассматриваться на уровне каждой группы, а не на уровне индивидуальных членов. Совет GNSO может также рассмотреть вопрос о приглашении представителей корпорации ICANN в качестве членов Постоянного комитета GNSO.

18.2.2. Сфера компетенции: Устав для Постоянного комитета GNSO должен быть разработан Советом GNSO совместно с консультативными комитетами, например GAC, SSAC и ALAC. Устав должен позволять комитету решать любые операционные вопросы, связанные с SSAD.

Это может включать, помимо прочего, такие темы, как соглашения об уровне обслуживания (SLA), централизация/децентрализация, автоматизация, цели третьих сторон, финансовая устойчивость и операционные/системные улучшения. Порог для включения вопроса в повестку дня Постоянного комитета GNSO должен быть достаточно низким, чтобы интересы любой из участвующих групп в деятельности SSAD серьезно учитывались в рамках комитета. Для определения вопросов, которые может решать комитет, будут использоваться два следующих способа:

i. Любая тема политики или реализации, касающаяся работы SSAD, может быть затронута членом Постоянного комитета GNSO и должна быть включена в рабочую повестку дня комитета, если это поддержит член комитета хотя бы еще от одной «группы».
ii. Кроме того, Совет GNSO может выявлять операционные проблемы SSAD. Совет GNSO может поручить Постоянному комитету GNSO оценить выявленные проблемы и представить Совету согласованные рекомендации заинтересованных сторон о том, как лучше всего их решать.

Рекомендации относительно принципов реализации должны быть отправлены в Совет GNSO для рассмотрения и принятия, после чего они передаются корпорации ICANN для выполнения дальнейшей работы по реализации. Рекомендации, которые требуют внесения изменений в действующую согласованную политику ICANN, должны регистрироваться и сохраняться для будущего использования на этапе определения нерешенных проблем в рамках разработки и (или) пересмотра политики.

18.2.3. Требуемый консенсус: Уровень согласия по рекомендациям Постоянного комитета GNSO: Чтобы отправить Совету GNSO официальные рекомендации по вопросам функционирования и политики SSAD, члены Постоянного комитета должны прийти к консенсусу по этим рекомендациям. Для достижения консенсуса по рекомендациям потребуется поддержка сторон, связанных договорными обязательствами. В целях оценки уровня консенсуса члены комитета должны представлять официальную позицию своих SG/C или SO/AC, а не свои личные взгляды или позиции. Для целей определения уровня консенсуса каждая из девяти групп, обеспечивающих консенсус, должна иметь равный вес при условии, что CP должны поддерживать конкретные рекомендации.

18.2.4. Роспуск Постоянного комитета GNSO: Постоянный комитет может рекомендовать Совету GNSO распустить самого себя, если возникнет такая необходимость. Для того, чтобы Постоянный комитет

рекомендовал Совету GNSO распустить его, при голосовании необходимо простое большинство участвующих групп. Эту рекомендацию впоследствии должен будет принять Совет GNSO.

3.6 Рекомендации Группы по EPDP с приоритетом 2

Recommendation #19. Отображение информации аффилированных и (или) аккредитованных провайдеров услуг сохранения конфиденциальности/регистрации через доверенных лиц

19.1. Если при регистрации доменного имени используется услуга аффилированной и (или) аккредитованной организации по сохранению конфиденциальности/регистрации через доверенных лиц (например, когда скрываются данные о физическом лице), регистратор (и, при необходимости, регистратура) ДОЛЖЕН включить в ответ на запрос RDDS полный набор данных RDDS соответствующего провайдера услуг сохранения конфиденциальности/регистрации через доверенных лиц. Полные данные RDDS провайдера услуг сохранения конфиденциальности/регистрации через доверенных могут также содержать переведенный в анонимную форму адрес электронной почты.

Замечания по реализации:

19.2. После реализации корпорацией ICANN программы аккредитации провайдеров услуг сохранения конфиденциальности и регистрации через доверенных лиц эта рекомендация № 19 заменит рекомендацию № 14 фазы 1 EPDP.

19.3. Цель этой рекомендации — дать регистраторам (и регистратурам, если применимо) следующее четкое указание: при регистрации домена через аффилированного и (или) аккредитованного провайдера услуг сохранения конфиденциальности/регистрации через доверенных лиц, эти данные НЕ ДОЛЖНЫ вымарываться. Рабочая группа предполагает, что регистрационные данные домена НЕ ДОЛЖНЫ одновременно вымарываться и скрываться через провайдера услуг сохранения конфиденциальности/регистрации через доверенных лиц.

Recommendation #20. Поле «город»

Группа по EPDP рекомендует обновить рекомендацию № 11 фазы 1 EPDP, чтобы указать, что применительно к контактным данным владельца домена поле «город» МОЖЕТ (а не ДОЛЖНО) вымарываться.

Recommendation #21. Хранение данных

Группа по EPDP подтверждает свою рекомендацию фазы 1 о том, что регистраторы ДОЛЖНЫ сохранять только те элементы данных, которые считаются необходимыми для целей TDRP, в течение пятнадцати месяцев после истечения срока действия регистрации плюс три месяца для осуществления процедуры удаления, то есть 18 месяцев. Основанием для такого срока хранения служит положение политики TDRP, согласно которому иск в рамках этой политики можно подать не позднее 12 месяцев после предполагаемого нарушения (сноска: см. раздел 2.2 TDRP) политики смены регистратора (сноска: см. раздел 1.15 TDRP). Настоящим поясняется, что это не лишает подателей запросов, включая отдел по контролю исполнения договорных обязательств ICANN, возможности запрашивать эти сохраненные элементы данных для целей, отличных от TDRP, но их раскрытие будет регулироваться соответствующими законами о защите данных, например, наличием правового основания для раскрытия данных. Во избежание разночтений настоящим поясняется, что указанный срок хранения не ограничивает возможность регистратур и регистраторов хранить элементы данных в течение большего срока.

Руководство по реализации:
Во избежание разночтений настоящим поясняется, что регистраторы обязаны хранить данные в течение 15 месяцев после прекращения действия регистрации и МОГУТ удалить эти данные по истечении 15-месячного срока.

Настоящим поясняется, что это не запрещает контроллерам вводить дополнительные периоды хранения для заявленных целей, которые определены и установлены контроллерами и отличаются от целей TDRP; это не исключает возможности раскрытия таких сохраненных данных любой стороне при условии соблюдения соответствующих законов о защите данных.

Recommendation #22. Цель № 2

Группа по EPDP рекомендует добавить следующую цель к целям фазы 1 Группы по EPDP, составляющим основу новой политики ICANN:

- Способствовать сохранению безопасности, стабильности и отказоустойчивости системы доменных имен в соответствии с миссией ICANN.

3.7 Выводы Группы по EPDP относительно приоритета 2

Вывод — цель OCTO
Рассмотрев этот комментарий, большинство членов Группы по EPDP пришло к соглашению, что на данном этапе нет необходимости предлагать дополнительную цель (цели), чтобы помочь офису технического директора (OCTO) ICANN в выполнении его миссии. Причина такого соглашения состоит в том, что недавно

обновленная Цель 2 ICANN в достаточной мере охватывает работу OCTO, наряду с работой других отделов корпорации ICANN, таких как отдел по контролю исполнения договорных обязательств и другие. Большинство также согласилось, что решение Группы по EPDP воздержаться от предложения дополнительных целей не помешает корпорации ICANN и (или) сообществу определить дополнительные цели для поддержки неуказанных будущих направлений деятельности, которые могут потребовать доступа к закрытым регистрационным данным.

Вывод — точность и система учета достоверности данных WHOIS
В соответствии с инструкциями Совета GNSO Группа по EPDP не будет больше рассматривать эту тему; вместо этого ожидается, что Совет GNSO сформирует аналитическую группу для дальнейшего изучения вопросов, касающихся точности и ARS, чтобы содействовать принятию решения о целесообразных последующих шагах для решения выявленных потенциальных проблем.

4 Дальнейшие действия

4.1 Дальнейшие действия

Настоящий итоговый отчет будет передан Совету GNSO для рассмотрения и утверждения. В случае принятия Советом GNSO итоговый отчет затем будет направлен в Правление ICANN для рассмотрения и, возможно, утверждения в качестве согласованной политики ICANN.

Глоссарий

1. Консультативный комитет
Консультативный комитет — официальный консультативный орган, состоящий из представителей интернет-сообщества, созданный для консультирования ICANN по конкретному вопросу или в конкретной области политики. Некоторые комитеты предусмотрены Уставом ICANN, другие могут создаваться по необходимости. Консультативный комитет не имеет полномочий действовать от лица ICANN, но может докладывать о своих результатах и давать рекомендации Правлению ICANN.

2. ALAC — Консультативный комитет At-Large
Консультативный комитет At-Large ICANN (ALAC) отвечает за обсуждение и предоставление рекомендаций по деятельности ICANN, затрагивающей интересы индивидуальных интернет-пользователей (сообщества At-Large). ICANN, как частная некоммерческая корпорация, отвечающая за техническое управление системой доменных имен и адресов интернета, опирается на ALAC и его вспомогательную инфраструктуру, чтобы вовлечь индивидуальных пользователей в деятельность ICANN и принять во внимание широкий круг их интересов.

3. Группа интересов коммерческих пользователей
Группа интересов коммерческих пользователей представляет интересы коммерческих пользователей интернета. Группа интересов коммерческих пользователей — одна из групп интересов, входящих в состав Группы коммерческих заинтересованных сторон (CSG), которая упоминается в статье 11.5 Устава ICANN. BC — одна из групп заинтересованных сторон и групп интересов Организации поддержки доменов общего пользования (GNSO), на которую возложена обязанность давать Правлению ICANN рекомендации по вопросам политики, относящимся к управлению системой доменных имен.

4. ccNSO — Организация поддержки национальных доменов
ccNSO является организацией поддержки, которая отвечает за выработку и передачу Правлению ICANN рекомендаций по глобальной политике в отношении национальных доменов верхнего уровня. Она выступает в качестве форума для регистратур национальных доменов верхнего уровня, где они могут встречаться и обсуждать важные проблемы на глобальном уровне. ccNSO избирает одного члена Правления.

5. ccTLD — национальный домен верхнего уровня
ccTLD — это домены, состоящие из двух букв, например .UK (Великобритания), .DE (Германия) и .JP (Япония). Они называются национальными доменами верхнего уровня (ccTLD) и соответствуют стране, территории или другому географическому местоположению. Правила и политика регистрации доменных

имен в ccTLD значительно разнятся, и регистратуры ccTLD разрешают использовать ccTLD только жителям соответствующей страны.

Дополнительную информацию о ccTLD, включая полную базу данных выделенных ccTLD и назначенных администраторов см. здесь: http://www.iana.org/cctld/cctld.htm.

6. Регистрационные данные доменного имени
Регистрационные данные доменного имени (их также называют регистрационными данными) — это информация, которую предоставляют при регистрации доменного имени владельцы доменов и собирают регистраторы или регистратуры. Некоторые из этих данных становятся общедоступными. Что касается взаимодействия между аккредитованными ICANN регистраторами и владельцами доменов общего пользования верхнего уровня (gTLD), элементы данных указаны в действующей редакции RAA. Для национальных доменов верхнего уровня (ccTLD) операторы этих TLD определяют политику запроса и отображения регистрационных данных самостоятельно или в соответствии с указаниями соответствующего правительства.

7. Доменное имя
В системе доменных имен доменные имена служат идентификаторами ресурсов интернет-протокола, например интернет-сайтов.

8. DNS — система доменных имен
DNS — это система доменных имен интернета. Система доменных имен (DNS) помогает пользователям ориентироваться в интернете. У каждого компьютера в интернете есть свой уникальный адрес — как номер телефона — и он состоит из довольно сложной строки цифр. Этот адрес называется IP-адресом (сокращение IP означает «интернет-протокол»). IP-адреса трудно запомнить. Система DNS упрощает использование интернета, позволяя вводить строку из букв (доменное имя) вместо непонятного IP-адреса. Поэтому вместо того чтобы вводить цифры 207.151.159.3, можно ввести www.internic.net. Это мнемонический способ, облегчающий запоминание адресов.

9. EPDP — Ускоренный процесс формирования политики GNSO
Ряд формальных этапов, описанных в Уставе ICANN и направленных на инициирование разработки, внутренний и внешний анализ, составление графика выработки и одобрения политики, необходимой для координации глобальной системы уникальных идентификаторов интернета. EPDP может начаться по инициативе Совета GNSO только в следующих особых ситуациях: (1) решение узкого вопроса политики, который выявлен и определен либо после одобрения Правлением ICANN рекомендации GNSO по политике, либо во время реализации такой одобренной рекомендации; или (2) предоставление новых или дополнительных рекомендаций по конкретному вопросу политики, который

практически определен ранее и по которому уже имеется обширная и уместная вспомогательная информация, например (а) отчет о неразрешенных проблемах для возможного PDP, который не был инициирован; (б) материалы предыдущего незавершенного PDP; (в) другие проекты, такие как Методологический процесс GNSO.

10. GAC — Правительственный консультативный комитет
GAC — консультативный комитет, состоящий из назначенных представителей национальных правительств, многонациональных правительственных организаций и организаций договора, а также обособленных экономических регионов. Его функция заключается в консультировании Правления ICANN по вопросам, относящимся к деятельности правительств. GAC служит форумом для обсуждения правительственных интересов и проблем, включая интересы потребителей. Как и любой другой консультативный комитет, GAC не уполномочен действовать от лица ICANN, но может докладывать о своих выводах и давать рекомендации Правлению ICANN.

11. Общий регламент по защите данных (GDPR)
Общий регламент по защите данных (ЕС) 2016/679 (GDPR) — нормативный акт ЕС о защите данных и конфиденциальности всех граждан Европейского Союза (ЕС) и Европейской экономической зоны (ЕЭЗ). В нем также рассматриваются вопросы экспорта персональных данных за пределы ЕС и ЕЭЗ.

12. GNSO — Организация поддержки доменов общего пользования
Организация поддержки, которая отвечает за разработку и передачу Правлению ICANN рекомендаций по существенным принципам политики в отношении доменов общего пользования верхнего уровня. В ее состав входят представители регистратур gTLD, регистраторов gTLD, сторон, интересующихся вопросами интеллектуальной собственности, интернет-провайдеров, коммерческих и некоммерческих сторон.

13. Домен общего пользования верхнего уровня (gTLD)
gTLD — это домен верхнего уровня в DNS, делегированный корпорацией ICANN согласно имеющему полную юридическую силу соглашению об администрировании домена верхнего уровня, не являющийся национальным TLD (ccTLD) или интернационализированным доменным именем (IDN-доменом) национального TLD.

14. Группа заинтересованных сторон-регистратур gTLD (RySG)
Группа заинтересованных сторон-регистратур gTLD (RySG) является признанной организацией в составе Организации поддержки доменов общего пользования (GNSO), созданной в соответствии с разделом 5 статьи X (сентябрь 2009 года) Устава Интернет-корпорации по присвоению имен и номеров (ICANN).

Основная функция RySG — представлять интересы операторов регистратур gTLD (или спонсоров в случае спонсируемых gTLD) («Регистратуры»), которые (i) заключили договор с ICANN об оказании услуг регистратуры gTLD для обеспечения работы одного или нескольких gTLD; (ii) согласились в этом договоре соблюдать согласованную политику; iii) решили стать членами RySG. RySG может включать группы интересов в соответствии со статьей IV. Группа RySG доводит мнения RySG до сведения Совета GNSO и Правления ICANN, уделяя особое внимание согласованной политике ICANN, относящейся к функциональной совместимости, технической надежности и (или) стабильному функционированию интернета или системы доменных имен.

15. ICANN — Интернет-корпорация по присвоению имен и номеров
Интернет-корпорация по присвоению имен и номеров (ICANN) — международная некоммерческая корпорация, которая несет ответственность за распределение адресного пространства интернет-протокола (IP-адресов), назначение идентификаторов протокола, управление системой доменных имен доменов общего пользования верхнего уровня (gTLD) и национальных доменов верхнего уровня (ccTLD), а также за функции управления системой корневых серверов. Первоначально ответственность за оказание данных услуг несли Администрация адресного пространства интернета (IANA) и другие организации согласно контракту с правительством США. Сейчас функции IANA выполняет ICANN. Как частно-государственное партнерство ICANN занимается защитой операционной стабильности интернета, продвижением конкуренции, обеспечением широкого представительства глобальных сообществ интернета и разработкой политики, соответствующей ее миссии посредством процесса, осуществляемого по принципу «снизу-вверх» и на основании консенсуса.

16. Группа интересов по вопросам интеллектуальной собственности (IPC)
Группа интересов по вопросам интеллектуальной собственности (IPC) представляет в ICANN мнения и интересы всемирного сообщества, занимающегося вопросами интеллектуальной собственности, уделяя особое внимание защите товарных знаков, авторского права и соответствующих прав на интеллектуальную собственность, а также вопросам их влияния на систему доменных имен (DNS) и взаимодействия с этой системой. IPC — одна из групп интересов Организации поддержки доменов общего пользования (GNSO), на которую возложена обязанность давать Правлению ICANN рекомендации по вопросам политики, относящимся к управлению системой доменных имен.

17. Группа интересов интернет-провайдеров и провайдеров связи (ISPCP)
Группа интересов интернет-провайдеров и провайдеров связи (ISPCP) — это группа интересов, входящая в состав GNSO. Цель этой группы интересов — выполнение функций и обязанностей, которые зафиксированы в соответствующих положениях уставов ICANN и GNSO, соблюдение политики или правил, которые корпорация ICANN принимает в результате своей деятельности.

ISPCP обеспечивает, чтобы мнения интернет-провайдеров и провайдеров связи вносили вклад в достижение целей и выполнение задач ICANN.

18. DNS-сервер
DNS-сервер — это компонент системы доменных имен, который хранит информацию об одной зоне (или нескольких зонах) пространства имен DNS.

19. Группа некоммерческих заинтересованных сторон (NCSG)
Группа некоммерческих заинтересованных сторон (NCSG) — это группа заинтересованных сторон, входящая в состав GNSO. Цель Группы некоммерческих заинтересованных сторон (NCSG) — представлять через избранных представителей и свои группы интересов проблемы и интересы владельцев доменов и интернет-пользователей доменов общего пользования верхнего уровня gTLD, не занимающихся коммерческой деятельностью. Она дает возможность высказать свое мнение и направить представителей для участия в процессах ICANN следующим лицам: некоммерческие организации, которые служат некоммерческим интересам или оказывают услуги некоммерческого характера в сфере образования, благотворительности, защиты потребителей, создания местных общественных организаций, поддержки искусства, защиты принципов общественной политики, благополучия детей, религии, научных исследований и прав человека; некоммерческие организации, которые отстаивают общественные интересы в области разработки программного обеспечения; семьи или физические лица, которые регистрируют доменные имена для личного некоммерческого использования; интернет-пользователи, которые проявляют особый интерес к некоммерческим аспектам политики в отношении доменных имен, имеющим отношение к общественным интересам.

20. Процедуры разрешения разногласий после делегирования (PDDRP)
Процедуры разрешения разногласий после делегирования были разработаны, чтобы у сторон, пострадавших в результате действий оператора регистратуры нового gTLD, была альтернативная возможность подачи жалобы на такие действия. Такие процедуры разрешения разногласий проводятся внешними поставщиками, независимыми от ICANN, и могут потребовать, чтобы истец предпринял конкретные шаги по решению своих проблем до подачи официальной жалобы. Экспертная комиссия определяет, совершил ли оператор регистратуры нарушение, и рекомендует ICANN меры по исправлению ситуации.

21. Зарегистрированное имя
«Зарегистрированное имя» означает доменное имя в gTLD, состоящее из двух (2) или более (например, john.smith.name) уровней, о котором оператор регистратуры gTLD (или его аффилированная организация или подрядчик, участвующий в оказании услуг регистратуры) хранит данные в базе данных регистратуры, организует такое хранение или получает доходы от такого хранения. Имя в базе данных регистратуры может быть зарегистрированным

именем, даже если оно не внесено в файл зоны (например, зарегистрированное, но неактивное доменное имя).

22. Регистратор
Слово «регистратор», начинающееся со строчной буквы, означает физическое или юридическое лицо, которое вступает в договорные отношения с владельцами зарегистрированных имен и оператором регистратуры, собирает регистрационные данные владельцев зарегистрированных имен и передает регистрационную информацию для занесения в базу данных регистратуры.

23. Группа заинтересованных сторон-регистраторов (RrSG)
Группа заинтересованных сторон-регистраторов — это одна из нескольких групп заинтересованных сторон сообщества ICANN, которая является представительным органом регистраторов. Это разнообразная и активная группа, работа которой направлена на эффективную защиту интересов регистраторов и их клиентов. Мы предлагаем вам подробнее узнать об аккредитованных регистраторах доменных имен и важных функциях, которые они выполняют в системе доменных имен.

24. Оператор регистратуры
«Оператор регистратуры» — это физическое или юридическое лицо, которое отвечает за оказание услуг регистратуры для конкретного gTLD в соответствии с соглашением между ICANN (или ее правопреемником) и этим физическим или юридическим лицом (этими физическими или юридическими лицами) или, если такое соглашение расторгнуто или его срок действия завершился, в соответствии с соглашением между правительством США и этим физическим или юридическим лицом (этими физическими или юридическими лицами).

25. Служба каталогов регистрационных данных (RDDS)
Служба каталогов регистрационных данных доменных имен или RDDS — это служба, предлагаемая (службы, предлагаемые) регистратурами и регистраторами для доступа к регистрационным данным доменных имен.

26. Процедура разрешения споров по ограничениям регистрации (RRDRP)
Процедура разрешения споров по ограничениям регистрации (RRDRP) предназначена для использования в ситуациях, когда оператор регистратуры нового gTLD от сообщества не соблюдает ограничения регистрации, изложенные в его Соглашении об администрировании домена верхнего уровня.

27. SO — организации поддержки
SO — это три специальных консультативных органа, которые дают Правлению ICANN рекомендации по вопросам, касающимся доменных имен (GNSO и CCNSO) и IP-адресов (ASO).

28. SSAC — Консультативный комитет по безопасности и стабильности
Консультативный комитет Правления ICANN, в состав которого входят технические эксперты из отрасли и сектора науки и образования, а также операторы корневых серверов интернета, регистраторы и регистратуры TLD.

29. TLD — домен верхнего уровня
TLD — это имена верхнего уровня в иерархии имен DNS. Они отображаются в доменных именах как набор символов за последней (крайней справа) точкой, например «net» вhttp://www.example.net. Администратор TLD контролирует, какие доменные имена второго уровня распознаются в этом TLD. Администратор «корневого домена» или «корневой зоны» контролирует, какие TLD распознаются системой DNS. К широко используемым TLD относятся .COM, .NET, .EDU, .JP, .DE и так далее.

30. Единая политика разрешения споров о доменных именах (UDRP)
Единая политика разрешения споров о доменных именах (UDRP) — это механизм защиты прав, который устанавливает процедуры и правила, применяемые регистраторами при возникновении споров в связи с регистрацией и использованием доменных имен в gTLD. UDRP обеспечивает наличие малозатратной административной процедуры, в результате которой принимаются обязательные для исполнения решения, предназначенной для урегулирования претензий в связи со злонамеренной, недобросовестной регистрацией доменных имен. Она применяется только к спорам между владельцами доменов и третьими сторонами, но не к спорам между регистратором и его клиентом.

31. Служба быстрой приостановки (URS)
Служба быстрой приостановки — это механизм защиты прав, который дополняет существующую Единую политику разрешения споров о доменных именах (UDRP), предоставляя правообладателям, столкнувшимся с наиболее очевидными случаями нарушения своих прав, менее дорогостоящий и более быстрый способ решения проблемы.

32. WHOIS
Протокол WHOIS — это протокол интернета, который используется для отправки запросов к базам данных с целью получения регистрационных данных доменного имени (или IP-адреса). Первоначально протокол WHOIS был определен в документе RFC 954, опубликованном в 1985 году. Документом действующей спецификации является RFC 3912. Соглашения ICANN с gTLD требуют, чтобы регистратуры и регистраторы предлагали интерактивную веб-страницу и услугу WHOIS через порт 43 с бесплатным открытым доступом к сведениям о зарегистрированных именах. Эти сведения обычно называются «данными WHOIS» и включают такие элементы, как дата регистрации и дата окончания срока регистрации доменного имени, DNS-серверы, контактные данные владельца

домена и назначенных контактных лиц по административным и техническим вопросам.

Службы WHOIS в основном используются для идентификации личности владельцев доменов в бизнес-целях и для определения сторон, способных устранить проблемы, связанные с зарегистрированным доменом.

Приложение A. Система обеспечения стандартизованного доступа к закрытым регистрационным данным и их раскрытия — вводная информация

ОПИСАНИЕ ПРОБЛЕМ И (ИЛИ) ВОПРОСЫ УСТАВА ГРУППЫ

Устав Группы по EPDP гласит:
(a) Цели доступа к данным — Какие вопросы политики, оставшиеся без ответа, будут определять реализацию?

a1) Каковы легитимные цели доступа третьих сторон к регистрационным данным в рамках применимого законодательства?
a2) Какие существуют правовые основы для поддержки этого доступа?
a3) Каковы квалификационные критерии для доступа третьих сторон к закрытым регистрационным данным?
a4) Состоят ли эти стороны/группы из разнотипных сторонних подателей запросов?
a5) К каким элементам данных должен получать доступ каждый пользователь/сторона, исходя из своих целей?
a6) В какой степени мы можем определить набор элементов данных и потенциальный спектр (объем) для конкретных третьих сторон и (или) целей?
a7) Как RDAP, обладающий техническими возможностями, может позволить регистратурам/регистраторам принимать токены аккредитации и цель запроса? После того, как модели аккредитации будут разработаны соответствующими органами по аккредитации и утверждены соответствующими юридическими органами, как мы можем гарантировать, что RDAP технически подготовлен и готов принимать, регистрировать и реагировать на токен аккредитованного подателя запроса?

(b) Получение учетных данных — Какие вопросы политики, оставшиеся без ответа, будут определять реализацию?

b1) Как будут предоставляться учетные данные и как ими управлять?
b2) Кто отвечает за предоставление учетных данных?
b3) Каким образом эти учетные данные будут интегрированы в технические системы регистраторов/регистратур?

(c) Условия доступа и соблюдение условий использования – Какие вопросы политики, оставшиеся без ответа, будут определять реализацию?

c1) Какие правила и политика будут регулировать доступ пользователей к данным?
c2) Какие правила и политика будут регулировать использование данных после предоставления доступа к ним?
c3) Кто будет отвечать за установление и обеспечение соблюдения этих правил и политики?
c4) С какими санкциями или штрафами за злоупотребление данными (если таковые имеются) столкнется пользователь, включая будущие ограничения на доступ или компенсацию для субъектов данных, чьи данные стали предметом злоупотреблений, в дополнение к любым санкциям, уже предусмотренным применимым законодательством?
c5) Какого рода понимание того, к каким данным осуществляется доступ и как они используются, получат стороны, связанные договорными обязательствами?
c6) Какие права имеют субъекты данных при определении того, когда и как к их данным предоставляется доступ и как они используются?
c7) Каким образом модель доступа третьей стороны может удовлетворить различные требования к уведомлению субъекта данных о раскрытии данных?

Из приложения к Временной спецификации:

- Разработка методов предоставления потенциальным истцам URS и UDRP достаточного доступа к регистрационным данным для поддержки подачи жалоб на принципах взаимного доверия
- Поиск баланса между ограничениями объема запросов, предусмотренными в программе аккредитации, и практическими потребностями перекрестных расследований.
- Конфиденциальность запросов на регистрационные данные со стороны правоохранительных органов
- Согласно Разделу 4.4, продолжение разработки сообществом модели аккредитации и обеспечения доступа, которая отвечает требованиям GDPR, с признанием необходимости получения дополнительных указаний от Рабочей группы 29-й статьи/Европейского совета по защите данных.
- Последовательный процесс бесперебойного доступа пользователей с легитимными целями к регистрационным данным, в том числе к закрытым данным, до тех пор пока не начнет полностью действовать итоговый механизм аккредитации и обеспечения доступа, обязательный для всех сторон, связанных договорными обязательствами.

Из итогового отчета Группы по EPDP о результатах фазы 1:

Рекомендация № 3 Группы по EPDP.
В соответствии со своим уставом и Целью № 2 Группа по EPDP теперь, когда есть ответы на вопросы устава, определяющие дальнейший подход, обязуется дать рекомендацию касательно стандартизованной модели законного раскрытия закрытых регистрационных данных (которая упоминается в уставе группы как «стандартизованный доступ»). Сюда входит решение таких вопросов, как:

- Следует ли внедрить такую систему?
- Каковы легитимные цели доступа третьих сторон к регистрационным данным?
- Каковы квалификационные критерии для доступа третьих сторон к закрытым регистрационным данным?
- Состоят ли эти стороны/группы из разнотипных сторонних подателей запросов?
- К каким элементам данных должен получать доступ каждый пользователь/сторона?

В данном контексте, помимо других вопросов, Группа по EPDP рассмотрит вопрос о раскрытии данных в случае незаконного использования интеллектуальной собственности и неправильного использования DNS. Необходимо убедиться, что раскрытие для легитимных целей не противоречит целям, для которых такие данные собраны.

Вопросы политики TSG

1. Результат EPDP или других инициатив в области политики доступа к закрытым регистрационным данным доменного имени gTLD.
2. Определение и выбор провайдеров идентификации (если этот выбор сделан), которые могут предоставлять учетные данные для использования в системе.[45]
3. Описание общих требований к подателю запроса, имеющему право доступа к закрытым данным регистрации доменного имени gTLD, например какие категории подателей запроса получают доступ к закрытым регистрационным данным доменного имени gTLD («политика авторизации») и к каким именно полям.
4. Детализация того, могут ли конкретные категории подателей запросов или податели запросов в целом скачивать журналы своей активности.
5. Описание требований к хранению данных, предъявляемых к каждому компоненту системы.

[45] Некоторые отметили, что этот вопрос может не входить в компетенцию Группы по EPDP.

6. Описание требований к уровню обслуживания (SLR) для каждого компонента системы, включая то, публикуются ли эти SLR и оценки их выполнения операторами компонентов, а также требований к обработке жалоб на доступ.
7. Определение законных причин для отклонения запроса.
8. Описание поддержки корреляции с помощью запроса об использовании псевдонима, как указано в разделе 7.2.
9. Описание выбранной модели субъекта, как указано в разделе 8, и соответствующие поддерживаемые компоненты и обнаружение служб, как описано в разделах с 10.1 по 10.5.
10. Описание условий, если таковые имеются, при которых запросы будут раскрыты CP.
11. Выполнение правового анализа ответственности операторов различных компонентов системы.
12. Описание процедуры подачи жалоб на неправомерное раскрытие информации и, соответственно, политики допустимого использования.

ОЖИДАЕМЫЙ ОТЧЕТ

Рекомендации по политике для стандартизованной модели законного доступа к закрытым регистрационным данным и их раскрытия

ОБЯЗАТЕЛЬНО К ПРОЧТЕНИЮ (ОБЩИЕ СВЕДЕНИЯ)

Описание	**Ссылка**	**Причина статуса «обязательно»**
Элементы концепции унифицированной модели непрерывного доступа к полным данным WHOIS (18 июня 2018 года)	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-18jun18-en.pdf	
Проект модели аккредитации и доступа к закрытым данным WHOIS (BC/IPC)	Версия 1.7 модели от 23 июля 2018 года	

Модель дифференцированного доступа к данным владельцев доменов Palage (также известная как Philly Special)	Модель дифференцированного доступа к данным владельцев доменов Palage (также известная как Philly Special) — версия 2.0 от 30 мая 2018 года	
Унифицированная модель непрерывного доступа к полным данным WHOIS — сравнение моделей, представленных сообществом (18 июня 2018 года)	https://www.icann.org/en/system/files/files/draft-unified-access-model-summary-elements-18jun18-en.pdf	
Мнение Рабочей группы 29-й статьи 2/2003 относительно применения принципов защиты данных к каталогам WHOIS (2003 год)	https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp76_en.pdf	
Отчет РГЭ, раздел 4c, Принципы аккредитации пользователей RDS (июнь 2014 года)	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf	
Исследование РГЭ — запрос информации об аккредитации пользователя RDS	https://community.icann.org/download/attachments/45744698/EWG%20USER%20ACCREDITATION%20RFI%20SUMMARY%2013%20March%202014.pdf	
Часть 1. Принципы работы: RDAP — 10 марта 2019 года	https://64.schedule.icann.org/meetings/963337	
Часть 2. Понимание RDAP и роли, которую он может играть в политике RDDS — 13 марта 2019 года	https://64.schedule.icann.org/meetings/961941	

Техническая исследовательская группа по доступу к закрытым регистрационным данным предложила Техническую модель доступа к закрытым регистрационным данным (30 апреля 2019 года)	TSG01, Техническая модель доступа к закрытым регистрационным данным	
Итоговый отчет по проблемам аккредитации провайдеров услуг сохранения конфиденциальности и регистрации через доверенных лиц (7 декабря 2015 года) ● Определения — стр. 6–8 ● Приложение B. Типичная концепция разглашения сведений по запросам со стороны владельцев прав на интеллектуальную собственность — стр. 85–93 ● Проект соглашения об аккредитации провайдеров услуг сохранения конфиденциальности и регистрации через доверенных лиц	https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf	

НЕОБХОДИМЫЕ БРИФИНГИ

Тема	Возможные докладчики	Причина важности
RDAP — встреча в формате «вопрос-ответ» для подведения итогов заседаний на ICANN65	Франциско Ариас (Francisco Arias), корпорация ICANN	Обеспечить общее понимание принципов работы и возможностей RDAP

ВЗАИМОЗАВИСИМЫЕ ЭЛЕМЕНТЫ

Опишите зависимость	Зависит от	Ожидаемые или рекомендуемые сроки
Переговоры и окончательное согласование соглашений о защите данных, требуемых в соответствии с отчетом фазы 1, являются предварительным условием для большей части работы на фазе 2 (предложено ISPCP).	СР/корпорация ICANN	

ПРЕДЛАГАЕМЫЕ СРОКИ И ПОДХОД

Введение
Задача Группы по EPDP — разработать и согласовать рекомендации по политике раскрытия закрытых регистрационных данных[46] запрашивающим сторонам (Система обеспечения стандартизованного доступа к закрытым регистрационным данным и их раскрытия).

До тех пор, пока соответствующие стороны не будут удовлетворены

[46] Из итогового отчета по фазе 1 EPDP: «Регистрационные данные» означают элементы данных, указанные в Приложении D [итогового отчета по фазе 1 EPDP], получаемые от физического и юридического лица в связи с регистрацией доменного имени.

юридическими гарантиями, разработка рекомендаций по политике для Системы обеспечения стандартизованного доступа к закрытым регистрационным данным и их раскрытия не будет зависеть от модели Системы.

Параллельно Группе по EPDP в целом следует взаимодействовать с корпорацией ICANN в разработке вопросов политики, которые помогут предоставить информацию для дискуссий с DPA, целью которых является определение того, какая модель системы стандартизованного раскрытия будет полностью соответствовать GDPR, будет работоспособной, а также сможет устранить или уменьшить юридическую ответственность сторон, связанных договорными обязательствами.

Неполный список тем, которые предполагается рассмотреть:

- Терминология и рабочие определения
- Необходимые правовые рекомендации
- Требования, в том числе определение групп пользователей, критериев и критериев/содержания запроса
- Публикация процесса, критериев и необходимых запросов информации
- График работ по процессу
- Получение подтверждения
- Аккредитация
- Аутентификация и авторизация
- Цели раскрытия данных третьим сторонам
- Правовое основание для раскрытия данных
- Политика допустимого использования
- Условия использования/соглашения о раскрытии данных, в том числе выполнение требований законодательства
- Политика конфиденциальности
- Политика запросов
- Хранение и уничтожение данных
- Соглашения об уровне обслуживания
- Финансовая устойчивость

Подход

Определить с самого начала следующее:

а) Терминология и рабочие определения
б) Перечень необходимых правовых рекомендаций (обратите внимание, что это также постоянная деятельность при рассмотрении всех тем).

Возможный логический порядок рассмотрения оставшихся тем:

в) Определить группы пользователей, критерии и цели/законное основание по каждой группе пользователей
↓
г) Аутентификация/авторизация/аккредитация групп пользователей
↓
д) Критерии/содержание запросов по каждой группе пользователей
↓
е) Политика запросов
↓
ж) Получение подтверждения, включая сроки
↓
з) Требования и ожидания в отношении ответов, включая сроки/SLA
↓
и) Политика допустимого использования
↓
к) Условия использования/соглашения о раскрытии данных/политика конфиденциальности
↓
л) Хранение и уничтожение данных

м) Общая тема для рассмотрения: финансовая устойчивость

Ниже приводится дополнительная информация по каждой из этих тем.
Чтобы перейти к каждому разделу, используйте ссылки ниже:

После заполнения этого и других рабочих листов каждая тема (включая темы фазы 1) и ее объем работы будут составлять основу общего рабочего плана с графиком выполнения. Некоторые темы могут рассматриваться параллельно, в то время как другие могут зависеть от другой работы, прежде чем можно будет провести более информированное обсуждение. По каждой теме будет предоставлено определенное время для обсуждения проблем, формулирования возможных выводов и (или) возможных рекомендаций по вопросам политики. Выводы или рекомендации, получившие общий уровень поддержки, будут переданы для дальнейшего рассмотрения и уточнения в рамках предварительного отчета. Цель состоит в том, чтобы достичь консенсуса по предложениям, где это возможно, до публикации.

a) Тема: Терминология и рабочие определения

Цель: Чтобы гарантировать одинаковое значение терминов, используемых в контексте этого обсуждения, и избежать путаницы, Группа по EPDP должна согласовать набор рабочих определений. Подразумевается, что эти рабочие определения служат только для пояснения используемой терминологии, они никоим образом не предназначены для ограничения объема работы или предопределения результата. Подразумевается, что эти рабочие определения необходимо будет пересмотреть и отредактировать, если потребуется, в конце процесса.

Материалы для рассмотрения:

- Терминология, используемая в GDPR и других законах о защите данных
- Итоговый отчет по проблемам аккредитации провайдеров услуг сохранения конфиденциальности и регистрации через доверенных лиц (7 декабря 2015 года) — Определения — стр. 6–8

Сопутствующий вопрос интеллект-карты: Нет

Сопутствующие аспекты выполнения рекомендаций фазы 1 EPDP: Подлежит уточнению — реализация рекомендации № 18 может включать определения, которые Группе по EPDP, возможно, потребуется учесть при обсуждениях на фазе 2.

Задачи:

- Подтвердить, предполагается ли разработка или применение каких-либо определений при выполнении рекомендации № 18 (персонал)
- Разработать первый проект рабочих определений. (персонал)
- Группа по EPDP должна провести анализ и внести предложения (EPDP)
- Согласовать базовый набор определений (EPDP)
- Ведение рабочего документа определений на основе обсуждений (все)

Срок завершения: 30 мая 2019 года

б) Тема: Правовые аспекты

Цель: определить правовые вопросы, ответы на которые необходимы Группе по EPDP для обсуждения этой темы.

Вопросы, представленные на сегодняшний день:

Вопрос	Статус	Исполнитель
1. Необходимо убедиться, что раскрытие для легитимных целей не противоречит целям, для которых такие данные собраны.	**ПРИОСТАНОВЛЕНО** LC фазы 2 отметил этот вопрос как преждевременный на данный момент и пометит его как «приостановленный». Вопрос будет повторно рассмотрен после того, как Группа по EPDP определит цели раскрытия данных.	
2. Ответить на вопрос о контроле и законном основании для системы стандартизованного доступа к закрытым регистрационным данным, исходя из предположения, что техническая концепция соответствует TSG, и таким образом, чтобы в достаточной мере решались проблемы, связанные с ответственностью и смягчением рисков с целью снижения рисков ответственности сторон, связанных договорными обязательствами, за счет внедрения системы стандартизованного доступа (IPC)	**ПЕРЕРАБОТАТЬ** LC фазы 2 переформулирует этот вопрос и после изучения обновленного текста определит, следует ли направить вопрос внешнему юрисконсульту.	
3. Следует запросить правовое заключение о возможности создания системы раскрытия данных на основе аккредитации как таковой. (ISPCP)	**ПРИОСТАНОВЛЕНО**	

	LC фазы 2 отметил этот вопрос как преждевременный на данный момент и пометит его как «приостановленный». Вопрос будет повторно рассмотрен после того, как Группа по EPDP определит цели раскрытия данных.	
4. Вопрос о раскрытии данных правоохранительным органам стран, не входящих в ЕС, на основании статьи 6 I f GDPR должен быть передан юрисконсульту. (ISPCP)	**ПЕРЕРАБОТАТЬ** LC фазы 2 ожидает дополнительной информации от автора этого вопроса и, после изучения такой информации и (или) обновленного текста определит, следует ли направить вопрос внешнему юрисконсульту.	
5. Может ли централизованная модель доступа к данным и их раскрытия (та, в которой одна организация отвечает за получение запросов о раскрытии данных, проверку сбалансированности интересов, проверку аккредитации, ответы на запросы и так далее) быть спроектирована таким образом, чтобы ограничить ответственность сторон, связанных договорными обязательствами, в максимально возможной степени? То есть допустимо ли предположить, что централизованная организация может нести основную (если не полную)	**ПЕРЕРАБОТАТЬ** LC фазы 2 переформулирует этот вопрос и после изучения обновленного текста определит, следует ли направить вопрос внешнему юрисконсульту.	

ответственность в связи с раскрытием данных (включая аккредитацию и авторизацию), и можно ли ограничить ответственность сторон, связанных договорными обязательствами, деятельностью, строго связанной с другой обработкой и не имеющей отношения к раскрытию данных, например со сбором и безопасной передачей данных? Если да, то что необходимо рассмотреть/сформулировать в политике для создания такой возможности? (ISPCP)		
6. В контексте SSAD, помимо определения собственного законного основания для раскрытия данных, нужно ли получающему запрос лицу (субъекту, хранящему запрошенные данные) оценивать законное основание третьей стороны, подателя запроса? (Вопрос, поступивший на ICANN65 от GAC/IPC)	**ПЕРЕРАБОТАТЬ** LC фазы 2 переформулирует этот вопрос и после изучения обновленного текста определит, следует ли направить вопрос внешнему юрисконсульту.	
7. В какой степени, если таковая имеется, стороны, связанные договорными обязательствами, несут ответственность, если третья сторона искажает информацию о предполагаемой обработке, и как можно уменьшить эту ответственность? (BC)	**ПЕРЕРАБОТАТЬ** LC фазы 2 переформулирует этот вопрос и после изучения обновленного текста определит, следует ли направить вопрос внешнему юрисконсульту.	
8. BC предлагает Группе по EPDP разделить Цель № 2 на две отдельные цели:	**ПРИОСТАНОВЛЕНО** LC фазы 2 отметил этот вопрос как	

• Предоставление ICANN возможности поддерживать безопасность, стабильность и отказоустойчивость системы доменных имен в соответствии с миссией и Уставом ICANN посредством контроля и обработки регистрационных данных gTLD. • Предоставление третьим сторонам возможности решать проблемы защиты потребителей, кибербезопасности, интеллектуальной собственности, киберпреступности и неправильного использования DNS, связанного с использованием или регистрацией доменных имен. Необходимо проконсультироваться с юрисконсультом, чтобы определить, можно ли изменить цель 2 (как указано выше). Можно ли проконсультироваться с юрисконсультом, чтобы определить возможность изменения цели 2 (как указано выше) в рамках GDPR? Если приведенная выше формулировка невозможна, может ли юрисконсульт внести предложения по ее улучшению? (BC)	преждевременный на данный момент и пометит его как «приостановленный». Вопрос будет вновь рассмотрен после проведения консультаций Совета GNSO и Правления по следующим вопросам: Рекомендация № 1, завершение работы над Целью № 2.	
9. Возможен ли юридический анализ того, как должна проводиться проверка баланса в соответствии с пунктом 6(1)(f), и при каких обстоятельствах 6(1)(f) может возникать необходимость рассмотрения запроса вручную? (BC)	**ПЕРЕРАБОТАТЬ** LC фазы 2 переформулирует этот вопрос и после изучения обновленного текста определит, следует ли направить вопрос внешнему юрисконсульту.	

10. Если проверка вручную выполняется не для всех запросов, существует ли правовая методика определения категорий запросов (например, оперативное реагирование на атаку вредоносного ПО или установление связи с нарушителем прав на интеллектуальную собственность, не отвечающим на запросы), которые можно структурировать для уменьшения необходимости проверки вручную? (BC)	**ПЕРЕРАБОТАТЬ** LC фазы 2 переформулирует этот вопрос и после изучения обновленного текста определит, следует ли направить вопрос внешнему юрисконсульту.	
11. Можно ли проконсультироваться с юрисконсультом, чтобы определить, препятствуют ли GDPR расширенному доступу должным образом сертифицированных специалистов по кибербезопасности, которые согласились на применение соответствующих механизмов защиты? Если такой доступ не запрещен, может ли юрисконсульт привести примеры механизмов защиты (таких как псевдонимизация), которые следует рассмотреть? (BC)	**ПЕРЕРАБОТАТЬ** LC фазы 2 переформулирует этот вопрос и после изучения обновленного текста определит, следует ли направить вопрос внешнему юрисконсульту.	
12. Чтобы определить 6(1)(b) как цель обработки регистрационных данных, мы должны следовать рекомендациям B&B о том, что «необходимо потребовать, чтобы конкретная третья сторона или, по крайней мере, обработка данных третьей стороной была хотя бы в общих чертах уже известна субъекту данных на момент заключения контракта, и чтобы контролер, как контрагент, сообщал об этом субъекту данных до передачи данных третьему лицу» Компания B&B должна пояснить, почему она считает, что единственным	**ПЕРЕРАБОТАТЬ** LC фазы 2 переформулирует этот вопрос и после изучения обновленного текста определит, следует ли направить вопрос внешнему юрисконсульту.	

основанием для предоставления данных WHOIS является предотвращение неправильного использования DNS. Ее вывод в параграфе 10 не учитывает другие цели, указанные Группой по EPDP в рекомендации 1, и в любом случае следует учитывать недавнее признание ЕС того факта, что у ICANN есть широкая цель: «способствовать поддержанию безопасности, стабильности и отказоустойчивости системы доменных имен в соответствии с миссией ICANN», которая лежит в основе роли ICANN как «хранителя» системы доменных имен.		
13. Компания B&B должна сообщить, в какой степени применимо основание «общественные интересы» пункта 6(1)e GDPR в свете признания ЕС следующего момента: «Что касается формулировки второй цели, Европейская комиссия признает центральную роль и ответственность ICANN за обеспечение безопасности, стабильности и отказоустойчивости системы доменных имен интернета, которая тем самым действует в общественных интересах».	**ПЕРЕРАБОТАТЬ** LC фазы 2 переформулирует этот вопрос и после изучения обновленного текста определит, следует ли направить вопрос внешнему юрисконсульту.	

Задачи:

- Определить первоочередные вопросы для соответствующих тем фазы 2
- Согласовать подход и процесс утверждения для вопросов, возникающих в ходе обсуждения

Срок завершения: постоянная работа

в) Тема: Определить группы пользователей, критерии и цели/законное основание по каждой группе пользователей

Цель:

- Определить категории групп пользователей, которые могут запрашивать раскрытие закрытых регистрационных данных/доступ к ним, а также критерии, которые должны применяться для определения принадлежности физического или юридического лица к этой категории.
- Определить цели и законное основание для обработки данных по каждой группе пользователей
- Определить, может ли стандартизованная концепция фазы 2 включать запросы, уникальные для групп с большими зонами обслуживания, и каким образом. Оценить, могут ли те, кто не вписывается ни в одну из идентифицированных групп пользователей, все же запрашивать раскрытие/доступ посредством выполнения рекомендации № 18 или другими способами.

Сопутствующие вопросы интеллект-карты:

Р1-Устав-а
(а) Цели доступа к данным — Какие вопросы политики, оставшиеся без ответа, будут определять реализацию?

а1) Каковы легитимные цели доступа третьих сторон к регистрационным данным в рамках применимого законодательства?
а2) Какие существуют правовые основы для поддержки этого доступа?
а3) Каковы квалификационные критерии для доступа третьих сторон к закрытым регистрационным данным?
а4) Состоят ли эти стороны/группы из разнотипных сторонних подателей запросов?

Приложение к Временной спецификации:
3. Разработка методов предоставления потенциальным истцам URS и UDRP доступа к регистрационным данным в достаточном для добросовестной подачи жалоб объеме.

Рекомендации фазы 1
Рекомендация № 3 Группы по EPDP

- Каковы легитимные цели доступа третьих сторон к регистрационным данным?
- Каковы квалификационные критерии для доступа третьих сторон к закрытым регистрационным данным?
- Состоят ли эти стороны/группы из разнотипных сторонних подателей запросов?

Группа по EPDP обращается с просьбой, чтобы в начале обсуждения концепции стандартизованного доступа Группой по EPDP представитель РГ по PDP RPM осветил текущее состояние дел, чтобы Группа по EPDP смогла понять, способны ли рекомендации РГ повлиять на рассмотрение URS и UDRP в контексте обсуждения концепции стандартизованного доступа.

Следует обратить внимание, что цель № 2 — заполнитель, который включен на период дополнительной проработки вопроса доступа на 2-й фазе EPDP. Ожидается, что эта цель будет пересмотрена по окончании 2-й фазы работ. [Примечание персонала — связано с целями, но срок пересмотра цели № 2: по окончании 2-й фазы работ]

TSG-Итоговый-B № 3
3. Описание общих требований к подателю запроса, имеющему право доступа к закрытым данным регистрации доменного имени gTLD, например какие категории подателей запроса получают доступ к закрытым регистрационным данным доменного имени gTLD («политика авторизации») и к каким именно полям.

Материалы для рассмотрения:

Описание	**Ссылка**	**Причина статуса «обязательно»**
В конце июня 2017 года ICANN попросила стороны, связанные договорными обязательствами, и заинтересованные стороны определить типы пользователей и целевое назначение элементов данных, являющихся обязательными в соответствии с политикой и контрактами ICANN. Полученные индивидуальные ответы и их подборка представлены ниже.	Таблица потока данных, компиляция полученных ответов — текущая версия	Последняя попытка определить типы пользователей
В итоговом отчете РГЭ отражена неполная сводная информация о пользователях существующей системы WHOIS, включая тех, кто использует ее в конструктивных целях, и тех, кто	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf – стр. 20-25	

использует ее в злонамеренных целях. В соответствии с кругом обязанностей РГЭ, все эти пользователи были изучены для определения существующих и возможных будущих рабочих процессов и участвующих в них заинтересованных сторон.		
Анализ установленных целей и законного основания, которые Группа по EPDP определила на фазе 1	https://gnso.icann.org/en/drafts/epdp-gtld-registration-data-specs-final-20feb19-en.pdf (стр. 34-36 / 67-71)	
Соответствующие положения GDPR	Соответствующие положения GDPR — см. статью 6(1), статью 6(2) и декларативную статью 40	
Информационная страница ICO, посвященная законному основанию обработки данных	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/	

Сопутствующие аспекты выполнения рекомендаций фазы 1 EPDP:
Не ожидается

Задачи:

- Составить первый список категорий подателей запросов на основе исходных материалов. (персонал)
- Проверить список категорий подателей запросов и определить критерии правомочности. (все)
- Определить типы и сценарии злоупотреблений, чтобы сформулировать примеры использования, устанавливающие требования для каждого подателя запроса
- Определить цели и законное основание для обработки данных по каждой группе пользователей (все)

- Определить, может ли стандартизованная концепция фазы 2 включать запросы, уникальные для групп с большими зонами обслуживания, и каким образом. Оценить, могут ли те, кто не вписывается ни в одну из идентифицированных групп пользователей, все же запрашивать раскрытие/доступ посредством выполнения рекомендации № 18 или другими способами. (все)
- Убедиться, что все вопросы устава группы рассмотрены и задокументированы.

Срок завершения: 13 июня 2019 года
(Пересмотр Цели № 2 — по окончании 2-й фазы работ)

г) Аутентификация/авторизация/аккредитация групп пользователей

Цель:

- Установить, требуется ли аутентификация, авторизация и (или) аккредитация групп пользователей
    - Может ли модель аккредитации дополнить то, что реализовано в результате выполнения Рекомендации № 18 фазы 1 EPDP, или использоваться вместе с этим?
- Если да, установить принципы политики для аутентификации, авторизации и (или) аккредитации, включая ответы на такие вопросы, как:
    - должен ли аутентифицированный пользователь, запрашивающий доступ к закрытым данным WHOIS, сообщать свой законный интерес для каждого отдельного вопроса/запроса.
- Если нет, объяснить, почему нет, и какие последствия это может иметь для запросов, поступающих от определенных групп пользователей, если таковые имеются.

Сопутствующие вопросы интеллект-карты:

P1-Устав-a/b

(a) Цели доступа к данным — Какие вопросы политики, которые остались без ответа, будут определять реализацию?
a7) Как RDAP, обладающий техническими возможностями, может позволить регистратурам/регистраторам принимать токены аккредитации и цель запроса? После того, как модели аккредитации будут разработаны соответствующими органами по аккредитации и утверждены соответствующими юридическими органами, как мы можем гарантировать, что RDAP технически подготовлен и готов принимать, регистрировать и реагировать на токен аккредитованного подателя запроса?

(b) Получение учетных данных — Какие вопросы политики, которые остались без ответа, будут определять реализацию?
b1) Как будут предоставляться учетные данные и как ими управлять?
b2) Кто отвечает за предоставление учетных данных?
b3) Каким образом эти учетные данные будут интегрированы в технические системы регистраторов/регистратур?

Приложение к Временной спецификации

1. Согласно Разделу 4.4, продолжение разработки сообществом модели аккредитации и обеспечения доступа, которая отвечает требованиям GDPR, с признанием необходимости получения дополнительных указаний от Рабочей группы 29-й статьи/Европейского совета по защите данных.

TSG-Итоговый-B № 2

Определить и выбрать провайдеров идентификации (если этот выбор сделан), которые могут предоставлять учетные данные для использования в системе.

Материалы для рассмотрения:

Описание	**Ссылка**	**Причина статуса «обязательно»**
Идентификация и аутентификация в модели TSG	https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf стр. 23–24	
Итоговый отчет РГЭ — Принципы авторизации использования контактных лиц RDS и аккредитации пользователей RDS	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf стр. 39–40 и стр. 62–67	
Проект концепции возможной модели единого доступа для непрерывного доступа к полным данным WHOIS — как будут разрабатываться требования к аутентификации законных пользователей?	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf стр. 9–10, 10–11, 18, 23	

Сопутствующие аспекты выполнения рекомендаций фазы 1 EPDP:
Не ожидается.

Задачи:

- Просмотреть материалы, перечисленные выше, и обсудить перспективы аутентификации/авторизации. (EPDP)
- Подтвердить определения ключевых терминов «авторизация», «аккредитация» и «аутентификация»
- Определить полный список вопросов политики и обсудить каждый из них
- Определить возможные решения или предлагаемые рекомендации, если таковые имеются
- Убедиться, что все вопросы устава группы рассмотрены и задокументированы.

Срок завершения: ICANN65

д) Критерии/информационное наполнение запросов по каждой группе пользователей

Цель: установить минимальные требования политики, критерии и содержание запросов по каждой группе пользователей, как указано в «с».

Сопутствующие вопросы интеллект-карты:

Р1-Устав-с
с1) Какие правила и политика будут регулировать доступ пользователей к данным?

Материалы для рассмотрения:

Описание	**Ссылка**	**Причина статуса «обязательно»**
• Приложение B. Типичная концепция разглашения сведений по запросам со стороны владельцев прав на интеллектуальную собственность — стр. 85–93 • Соглашение об аккредитации провайдеров услуг сохранения конфиденциальности и регистрации через доверенных лиц	Итоговый отчет по проблемам аккредитации провайдеров услуг сохранения конфиденциальности и регистрации через доверенных лиц (7 декабря 2015 года)	
Пример: информация и форма запроса для домена .DE	https://www.denic.de/en/service/whois-service/third-party-requests-for-holder-data/ https://www.denic.de/fileadmin/public/downloads/Domaindatenanfrage/Antrag_Domaindate	

	n_Rechteinhaber_EN.pdf	
Пример: форма запроса Nominet	https://s3-eu-west-1.amazonaws.com/nominet-prod/wp-content/uploads/2018/05/22101442/Data-request-form.pdf	

Сопутствующие аспекты выполнения рекомендаций фазы 1 EPDP:

Рекомендация № 18 (но НЕ требует автоматического раскрытия данных)

Минимально необходимая информация в составе обоснованного запроса о раскрытии данных на законных основаниях:

- идентификационные данные и сведения о подателе запроса (включая характер/вид бизнеса юридического или физического лица и заявление о наличии полномочий, когда это применимо и уместно);
- информация о законных правах подателя запроса и конкретное обоснование и/или основание для запроса, (напр., что является основанием или причиной для запроса; для чего подателю запроса необходимы эти данные?);
- заверение в том, что это добросовестный запрос;
- список запрашиваемых элементов данных с указанием причин, по которым для удовлетворения потребностей подателя запроса необходимы именно эти данные;
- согласие выполнять только законную обработку любых данных, полученных в ответ на запрос.

Задачи:

- Подтвердить подход к реализации рекомендации № 18
- Подтвердить определения ключевых терминов
- Определить полный список вопросов политики и обсудить каждый из них
- Определить возможные решения или предлагаемые рекомендации, если таковые имеются
- Убедиться, что все вопросы устава группы рассмотрены и задокументированы.

Срок завершения: ICANN65

e) Политика запросов

Цель: Установить минимальные требования политики регистрации запросов, определив соответствующие элементы управления: когда должны быть доступны журналы запросов и требуется ли ввести ограничения для запросов аутентифицированных и не аутентифицированных пользователей SSAD.

- Как будет ограничиваться доступ к закрытым регистрационным данным, чтобы свести к минимуму риски несанкционированного доступа и использования (например, путем предоставления доступа только на основе конкретных запросов в отличие от массовой передачи данных и (или) других ограничений на поиск или использование службы обратных каталогов, включая механизмы ограничения доступа к полям только тем, что необходимо для достижения легитимной цели)?
- Следует ли учитывать конфиденциальность запросов, например, от правоохранительных органов?
- Как следует уравновесить ограничения по запросам и реальные потребности в перекрестных ссылках при расследовании?

Сопутствующие вопросы интеллект-карты:

P1-Устав-a
a7) Как RDAP, обладающий техническими возможностями, может позволить регистратурам/регистраторам принимать токены аккредитации и цель запроса? После того, как модели аккредитации будут разработаны соответствующими органами по аккредитации и утверждены соответствующими юридическими органами, как мы можем гарантировать, что RDAP технически подготовлен и готов принимать, регистрировать и реагировать на токен аккредитованного подателя запроса?

Приложение к Временной спецификации:
6 Поиск баланса между ограничениями объема запросов, предусмотренными в программе аккредитации, и реальными потребностями в перекрестных ссылках при расследовании.
7 Конфиденциальность запросов о раскрытии регистрационных данных со стороны правоохранительных органов.

Материалы для рассмотрения:

Описание	**Ссылка**	**Причина статуса «обязательно»**
SSAC 101 — Рекомендация SSAC относительно доступа к регистрационным данным доменных имен	https://www.icann.org/en/system/files/files/sac-101-en.pdf	Описывает последствия ограничений скорости.

Сопутствующие аспекты выполнения рекомендаций фазы 1 EPDP: Нет.

Задачи:

- Подтвердить определения ключевых терминов
- Определить полный список вопросов политики и обсудить каждый из них
- Определить возможные решения или предлагаемые рекомендации, если таковые имеются
- Убедиться, что все вопросы устава группы рассмотрены и задокументированы.

Срок завершения: ICANN65

ж) Подтверждение получения, включая сроки

Цель: Определить требования политики в отношении сроков подтверждения получения и дополнительных требований (если таковые имеются), которые должно содержать подтверждение.

Каковы (если таковые имеются) базовые минимальные стандартизованные требования к подтверждению получения для регистраторов/регистратур?
Что насчет «срочных» запросов и как они определяются?

Сопутствующие вопросы интеллект-карты:

P1-Устав-c
c1) Какие правила и политика будут регулировать доступ пользователей к данным?

Материалы для рассмотрения:

Описание	**Ссылка**	**Причина статуса «обязательно»**
Итоговый отчет по фазе 1, рекомендация № 18 Сроки и критерии ответов регистраторов и операторов регистратур	https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf стр. 19	

Сопутствующие аспекты выполнения рекомендаций фазы 1 EPDP:
— рекомендация № 18*:*
Сроки и критерии ответов регистраторов и операторов регистратур — регистраторы и регистратуры обязаны объективно рассматривать и выполнять запросы о раскрытии данных на законных основаниях:
• Срок подтверждения получения обоснованного запроса о раскрытии данных на законных основаниях. Без необоснованной задержки, но не более 2 (двух) рабочих дней после получения запроса, если не было продемонстрировано, что обстоятельства не позволяют этого сделать.

Задачи:
- Подтвердить определения ключевых терминов
- Определить полный список вопросов политики и обсудить каждый из них
- Определить возможные решения или предлагаемые рекомендации, если таковые имеются
- Убедиться, что все вопросы устава группы рассмотрены и задокументированы.

Срок завершения: Подлежит определению

з) Требования и ожидания в отношении ответов, включая сроки/SLA

Цель: Определить требования политики в отношении ответов, включая решение таких вопросов, как:

- включая решение таких вопросов, как:
    - Должны ли возвращаться полные данные WHOIS при выполнении запроса аутентифицированным пользователем?
    - Какими должны быть обязательства SLA для ответов на запросы о доступе/раскрытии?
    - Каковы минимальные требования к ответам на запросы, включая отклонение запросов?

Сопутствующие вопросы интеллект-карты:

P1-Устав-a/c
a5) К каким элементам данных должен получать доступ каждый пользователь/сторона, исходя из их цели?
a6) В какой степени мы можем определить набор элементов данных и потенциальный спектр (объем) для конкретных третьих сторон и (или) целей?
c1) Какие правила и политика будут регулировать доступ пользователей к данным?

Рекомендация фазы 1 — № 3
К каким элементам данных должен получать доступ каждый пользователь/сторона?

Приложение к Временной спецификации
2. Рассмотрение возможности обязать уникальных контактных лиц иметь единый обезличенный адрес электронной почты для всех доменных имен, зарегистрированных у конкретного регистратора, обеспечивая при этом безопасность/стабильность и выполняя требования раздела 2.5.1 Приложения A.

TSG-Итоговый-B № 6
Описание требований к уровню обслуживания (SLR) для каждого компонента системы, включая то, публикуются ли эти SLR и оценки их выполнения операторами компонентов, а также требований к обработке жалоб на доступ.
TSG-Итоговый-B № 7
Определение законных причин для отклонения запроса.
TSG-Итоговый-B № 8
Описание поддержки корреляции с помощью запроса об использовании псевдонима, как указано в разделе 7.2.

Материалы для рассмотрения:

Описание	**Ссылка**	**Причина статуса «обязательно»**
Итоговый отчет по фазе 1, рекомендация № 18 Сроки и критерии ответов регистраторов и операторов регистратур	https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf стр. 19	
Итоговый отчет по проблемам аккредитации провайдеров услуг сохранения конфиденциальности и регистрации через доверенных лиц (7 декабря 2015 года) ● Приложение B. Типичная концепция разглашения сведений по запросам со стороны владельцев прав на интеллектуальную собственность — стр. 90–92	https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf	Раздел PPSAI с концепцией раскрытия данных и подробным описанием необходимого минимального ответа

Сопутствующие аспекты выполнения рекомендаций фазы 1 EPDP*:*
Рекомендация № 18:

- Требования в отношении содержания ответа. Ответы на отклоненные (полностью или частично) запросы о раскрытии данных должны содержать: обоснование, достаточное для того, чтобы податель запроса понял причины принятого решения, в том числе, например, анализ и разъяснение

того, как проводилась проверка сбалансированности интересов (если применимо).

- Необходимо вести журналы запросов, подтверждений и ответов в соответствии с типовой практикой протоколирования деловых операций, чтобы они были доступны по мере необходимости, например, помимо прочего, для целей их проверки отделом ICANN по контролю исполнения договорных обязательств.
- Ответ на запрос необходимо дать без необоснованной задержки, при этом максимальный срок ответа в отсутствие исключительных обстоятельств составляет 30 дней. К таким обстоятельствам может относиться общее количество полученных запросов. Стороны, связанные договорными обязательствами, будут регулярно информировать ICANN о количестве поступивших запросов, чтобы можно было оценить обоснованность сроков ответа.
- Будет рассмотрена возможность введения отдельного срока ответа [менее X рабочих дней] на «Срочные» обоснованные запросы о раскрытии данных, в которых представлены доказательства необходимости срочно раскрыть информацию [окончательные временные рамки и критерии для срочных запросов должны быть определены на этапе реализации].

Задачи:

- Подтвердить определения ключевых терминов
- Определить полный список вопросов политики и обсудить каждый из них
- Определить возможные решения или предлагаемые рекомендации, если таковые имеются
- Убедиться, что все вопросы устава группы рассмотрены и задокументированы.

Срок завершения: август

и) Политика допустимого использования

Цель: Определить требования политики в отношении следующего:

1. Как следует разрабатывать, постоянно развивать и обеспечивать соблюдение кодекса поведения (если таковой необходим)?
2. Если ICANN и стороны, связанные с ней договорными обязательствами, разработают кодекс поведения для третьих сторон, имеющих законный интерес, какие особенности и потребности следует учитывать?
3. Существуют ли дополнительные потоки данных, которые необходимо документировать, помимо того, что было задокументировано на фазе 1? Может ли модель кодекса поведения дополнить то, что реализовано в результате выполнения рекомендации № 18 фазы 1 EPDP, или использоваться вместе с этим?

Сопутствующие вопросы интеллект-карты:

P1-Устав-с
c1) Какие правила и политика будут регулировать доступ пользователей к данным?
c2) Какие правила и политика будут регулировать использование данных после предоставления доступа к ним?
c3) Кто будет отвечать за установление и обеспечение соблюдения этих правил и политики?
c4) С какими санкциями или штрафами (если таковые имеются) за злоупотребление данными столкнется пользователь, включая будущие ограничения на доступ или компенсацию для субъектов данных, чьи данные стали предметом злоупотреблений, в дополнение к любым санкциям, уже предусмотренным применимым законодательством?
c5) Какого рода понимание того, к каким данным осуществляется доступ и как они используются, получат стороны, связанные договорными обязательствами?
c6) Какие права имеют субъекты данных при определении того, когда и как к их данным предоставляется доступ и как они используются?
c7) Каким образом модель доступа третьей стороны может удовлетворить различные требования к уведомлению субъекта данных о раскрытии данных?

Материалы для рассмотрения:

Описание	**Ссылка**	**Причина статуса «обязательно»**
GDPR, статья 40, Кодекс поведения	https://gdpr-info.eu/art-40-gdpr/	
Письмо Рабочей группы 29-й статьи в ICANN 11 апреля 2018 года	https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf	
Bird & Bird — Кодекс поведения и справочные материалы по сертификации (май 2017 года)	https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/43--guide-to-the-gdpr--codes-of-	

	conduct-and-certifications.pdf?la=en	
Пример: Кодекс поведения поставщиков облачных услуг (CISPE) (январь 2017 года)	https://cispe.cloud/code-of-conduct/	
Пример: Кодекс поведения поставщиков облачных услуг (облако ЕС) (ноябрь 2018 года)	https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html	

Сопутствующие аспекты выполнения рекомендаций фазы 1 EPDP: Нет.

Задачи:

- Определить полный список вопросов политики и обсудить каждый из них
- Определить возможные решения или предлагаемые рекомендации, если таковые имеются
- Убедиться, что все вопросы устава группы рассмотрены и задокументированы.

Срок завершения: август

к) Условия использования/соглашения о раскрытии данных/политика конфиденциальности

Цель: Определить требования политики в отношении условий использования для третьих лиц, которые хотят получить доступ к закрытым регистрационным данным:

- Как минимум, какие меры необходимы для надлежащей защиты персональных данных, которые могут быть предоставлены аккредитованному пользователю/третьей стороне?
- Какие процедуры должны быть установлены для доступа к данным?
- Какие процедуры должны быть установлены для ограничения использования данных, к которым осуществляется надлежащий доступ?

- Необходимы ли отдельные Условия использования для разных групп пользователей?
- Кто будет контролировать и обеспечивать соблюдение Условий использования?
- Какой механизм будет использован для контроля за соблюдением Условий использования?

Сопутствующие вопросы интеллект-карты:

P1-Устав-с
с1) Какие правила и политика будут регулировать доступ пользователей к данным?
с2) Какие правила и политика будут регулировать использование данных после предоставления доступа к ним?
с3) Кто будет отвечать за установление и обеспечение соблюдения этих правил и политики?
с4) С какими санкциями или штрафами (если таковые имеются) за злоупотребление данными столкнется пользователь, включая будущие ограничения на доступ или компенсацию для субъектов данных, чьи данные стали предметом злоупотреблений, в дополнение к любым санкциям, уже предусмотренным применимым законодательством?

TSG-Итоговый-B № 4
Детализация того, могут ли конкретные категории подателей запросов или податели запросов в целом скачивать журналы своей активности.
TSG-Итоговый-B № 10
Описание условий, если таковые имеются, при которых запросы будут раскрыты СР.
TSG-Итоговый-B № 11
Выполнение правового анализа ответственности операторов различных компонентов системы.
TSG-Итоговый-B № 12
Описание процедуры подачи жалоб на неправомерное раскрытие информации и, соответственно, политики допустимого использования

Материалы для рассмотрения:

Описание	**Ссылка**	**Причина статуса «обязательно»**
Проект концепции возможной модели единого доступа для непрерывного доступа к полным данным WHOIS – какова будет роль Условий использования в унифицированной модели доступа?	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf стр. 14-16	

Сопутствующие аспекты выполнения рекомендаций фазы 1 EPDP:

Задачи:

- Подтвердить определения ключевых терминов
- Определить полный список вопросов политики и обсудить каждый из них
- Определить возможные решения или предлагаемые рекомендации, если таковые имеются
- Убедиться, что все вопросы устава группы рассмотрены и задокументированы.

Срок завершения: сентябрь

л) Хранение и уничтожение данных

Цель: Установить минимальные требования политики для хранения, удаления и регистрации данных, сохраняемых для сторон, участвующих в SSAD, включая, помимо прочего, регистрационные данные gTLD, информацию об учетной записи пользователя, журналы транзакций и метаданные, такие как дата и время запросов.

Сопутствующие вопросы интеллект-карты:

P1-Устав-c
c2) Какие правила и политика будут регулировать использование данных после предоставления доступа к ним?

TSG-Итоговый-B № 5
Описание требований к хранению данных, предъявляемых к каждому компоненту системы.

Материалы для рассмотрения:

Описание	**Ссылка**	**Причина статуса «обязательно»**
GDPR, статья 5(1)(e)	https://gdpr.algolia.com/gdpr-article-5	
Хранение данных в модели TSG	https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf стр. 26	

Сопутствующие аспекты выполнения рекомендаций фазы 1 EPDP:
Рекомендация № 15:
1. Чтобы получить информацию, которая необходима для 2-й фазы работы, Группа по EPDP рекомендует корпорации ICANN в срочном порядке проанализировать все свои активные процессы и процедуры, чтобы определить и задокументировать случаи, когда регистратор запрашивает персональные данные по истечении срока регистрации. После этого следует определить и задокументировать сроки хранения конкретных элементов данных, чтобы опираться на эту информацию при установлении необходимых актуальных и конкретных минимальных требований к хранению данных регистраторами. Группа по EPDP рекомендует предложить членам сообщества внести вклад в эту работу по сбору данных, представив свои комментарии относительно других легитимных целей, для которых могут применяться различные периоды хранения.

2. Пока Группа по EPDP признала, что самый большой обоснованный срок хранения данных — один год — предусмотрен в Политике разрешения споров при изменении регистраторов (TDRP), и поэтому рекомендовала обязать регистраторов хранить только те элементы данных, которые необходимы для целей TDRP, в течение пятнадцати месяцев по окончании срока регистрации и еще три месяца до полного удаления, то есть 18 месяцев. Основанием для такого срока хранения служит положение политики TDRP, согласно которому иск в рамках этой политики можно подать не позднее 12 месяцев после предполагаемого нарушения (сноска: см. раздел 2.2 TDRP) политики смены регистратора (сноска: см. раздел 1.15 TDRP). Этот срок хранения не ограничивает

возможность регистратур и регистраторов хранить в течение боле короткого срока элементы данных, перечисленные в рекомендациях № 4–7, для других целей, которые указаны в рекомендации № 1.

3. Группа по EPDP признает, что у сторон, связанных договорными обязательствами, могут быть потребности или требования, обуславливающие необходимость других сроков хранения, отвечающих местному законодательству или иным требованиям. Группа по EPDP обращает внимание на то, что эта рекомендация или отдельная обязательная для соблюдения политика ICANN никоим образом не запрещает сторонам, связанным договорными обязательствами, устанавливать собственные сроки хранения, которые могут быть длиннее или короче тех, что определены в политике ICANN.

4. Группа по EPDP рекомендует, чтобы корпорация ICANN пересмотрела свою текущую процедуру получения разрешения на отступление от требования хранить данные для повышения ее эффективности, сокращения срока рассмотрения заявок и соблюдения GDPR. Например, если Регистратору из определенной юрисдикции разрешено не хранить данные, Регистраторы, находящиеся в аналогичной ситуации, могли бы воспользоваться этим разрешением через процедуру уведомления без необходимости подавать отдельную заявку по этой процедуре.

Задачи:

- Подтвердить определения ключевых терминов
- Определить полный список вопросов политики и обсудить каждый из них
- Определить возможные решения или предлагаемые рекомендации, если таковые имеются
- Убедиться, что все вопросы устава группы рассмотрены и задокументированы.

Срок завершения: сентябрь

м) Финансовая устойчивость

Цель: Гарантировать, что все аспекты SSAD являются финансово устойчивыми. Оценить, как и кто несет расходы на внедрение SSAD и управление ею.

- Определить, существовала ли рыночная неэффективность до мая 2018 года и существует ли она после выполнения рекомендаций фазы 1 EPDP.
- Должны ли стороны, связанные договорными обязательствами, и (или) ICANN нести расходы на стандартизованное решение, хотя считается, что раскрытие регистрационных данных отвечает общественным интересам?
- Если аккредитация является жизнеспособным решением, следует ли ввести соответствующие сборы за подачу заявления, или структура сборов должна основываться на типе (многоуровневая структура), размере или количестве раскрытых данных?
- Следует ли или можно ли субъектам данных получить компенсацию за раскрытие их данных?

Сопутствующие вопросы интеллект-карты: Нет

Материалы для рассмотрения:

Описание	**Ссылка**	**Причина статуса «обязательно»**

Сопутствующие аспекты выполнения рекомендаций фазы 1 EPDP: Нет

Задачи:

- Подтвердить определения ключевых терминов
- Определить полный список вопросов политики и обсудить каждый из них
- Определить возможные решения или предлагаемые рекомендации, если таковые имеются
- Убедиться, что все вопросы устава группы рассмотрены и задокументированы.

Срок завершения: Подлежит определению

Приложение B. Общие сведения

История процесса и вопроса

19 июля 2018 года Совет GNSO инициировал Ускоренный процесс формирования политики (EPDP) и учредил Группу по EPDP в области Временной спецификации для регистрационных данных в gTLD. В отличие от других PDP GNSO, в которых может участвовать любой, Совет GNSO решил ограничить членский состав Группы по EPDP, главным образом, исходя из необходимости выполнить работу в сравнительно короткий срок и ответственно подойти к выделению ресурсов на эту деятельность. Группам заинтересованных сторон GNSO, Правительственному консультативному комитету (GAC), Организации поддержки национальных доменов (ccNSO), Консультативному комитету At-Large (ALAC), Консультативному комитету системы корневых серверов (RSSAC) и Консультативному комитету по безопасности и стабильности (SSAC) было предложено назначить определенное количество членов и их дублеров, как указано в уставе. Кроме того, Правлению и корпорации ICANN было предложено назначить несколько представителей в состав этой группы. Для формирования вышеупомянутых групп в июле было опубликовано объявление о наборе волонтеров, и 1 августа 2018 года Группа по EPDP провела свое первое совещание в фазе 1.

История вопроса

17 мая 2018 года Правление ICANN приняло Временную спецификацию для регистрационных данных в gTLD. Правление сделало это, чтобы установить для ICANN и сторон, связанных договорными обязательствами, временные условия соблюдения действующих контрактных требований и выработанной сообществом политики в области WHOIS и одновременно обеспечить соблюдение Общего регламента по защите данных (GDPR) Европейского Союза (ЕС). Временная спецификация была принята согласно процедуре подготовки временных спецификаций, определенной Соглашением об администрировании домена верхнего уровня (RA) и Соглашением об аккредитации регистраторов (RAA). После утверждения Временной спецификации Правление «должно незамедлительно начать процесс разработки согласованной политики, который определен в Уставе ICANN».[47] Процесс разработки согласованной политики в области Временной спецификации должен быть выполнен за один год. Кроме того, одной из его задач является обсуждение системы стандартизованного доступа к закрытым регистрационным данным.

[47] См. раздел 3.1 (a) Соглашения об администрировании домена верхнего уровня: https://www.icann.org/resources/unthemed-pages/org-agmt-html-2013-09-12-en

На заседании 19 июля 2018 года Совет Организации поддержки доменов общего пользования (GNSO) запустил EPDP в области Временной спецификации для регистрационных данных в gTLD и принял устав Группы по EPDP. В отличие от других PDP GNSO, в которых может участвовать любой, Совет GNSO решил ограничить членский состав Группы по EPDP, главным образом, исходя из необходимости выполнить работу в сравнительно короткий срок и ответственно подойти к выделению ресурсов на эту деятельность. Группам заинтересованных сторон GNSO, Правительственному консультативному комитету (GAC), Организации поддержки национальных доменов (ccNSO), Консультативному комитету At-Large (ALAC), Консультативному комитету системы корневых серверов (RSSAC) и Консультативному комитету по безопасности и стабильности (SSAC) было предложено назначить определенное количество членов и их дублеров, как указано в уставе. Кроме того, Правлению и корпорации ICANN было предложено назначить несколько представителей в состав этой группы.

21 ноября 2018 года Группа по EPDP опубликовала свой первоначальный отчет по результатам работы в рамках фазы 1 для общественного обсуждения. Группа по EPDP включила комментарии общественности в итоговый отчет по фазе 1, и Совет GNSO проголосовал за принятие всех 29 рекомендаций итогового отчета по фазе 1 EPDP на своем заседании 4 марта 2019 года. 15 мая 2019 года Правление ICANN приняло итоговый отчет по фазе 1 группы EPDP, за исключением частей двух рекомендаций: 1) Цель № 2 в рекомендации № 1 и 2) возможность удаления данных в поле «Организация» в рекомендации № 12. В соответствии с Уставом ICANN между Советом GNSO и Правлением ICANN будут проведены консультации для обсуждения тех частей рекомендаций фазы 1 EPDP, которые не были приняты Правлением ICANN. В то же время группа по анализу реализации (IRT), состоящая из представителей корпорации ICANN и членов сообщества ICANN, теперь будет выполнять утвержденные рекомендации итогового отчета фазы 1 Группы по EPDP. Дополнительные сведения о статусе реализации см. здесь.

2 мая 2019 года Группа по EPDP начала фазу 2 своей работы. В круг задач фазы 2 EPDP входит: (i) обсуждение системы стандартизованного доступа к закрытым регистрационным данных и их раскрытия, (ii) вопросы, отмеченные в Приложении к Временной спецификации для регистрационных данных в gTLD («Важные вопросы, подлежащие дальнейшему рассмотрению сообществом») и (iii) неразрешенные вопросы, отложенные по результатам фазы 1, например вопрос юридических и физических лиц, вымарывание поля «город» и так далее. Дополнительная информация приведена здесь.

Приложение C. Состав Группы по EPDP и участие в заседаниях

Состав Группы по EPDP и участие в заседаниях

Сводка по работе на заседаниях:

Пленарные заседания:

- 75 пленарных заседаний (155,5 часа)
- 12 очных заседаний (77,5 часа)
- 01 вебинар (1,0 час)
- Суммарная доля участия 86%

Заседания малых групп:

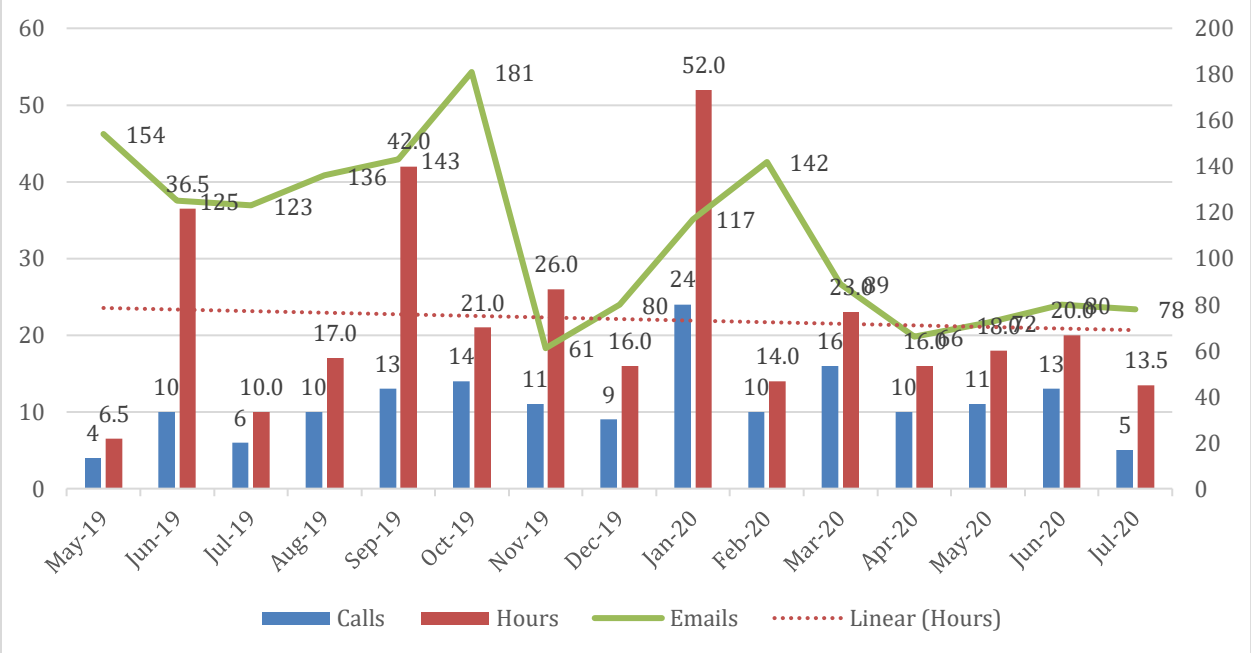
- 10 телеконференций в подгруппах (18,0 часов)

Заседания юридического комитета:

- 19 телеконференций в подгруппах (29,4 часа)
- 01 очное заседание (1,5 часа)

Заседания руководства:

- 48 телеконференций руководства (47,5 часа)
- 04 очных заседания руководства (20,5 часа)



С подробным списком, SOI и посещаемостью можно ознакомиться на странице https://community.icann.org/x/kBdIBg.

Архив электронной почты размещен по адресу https://mm.icann.org/pipermail/gnso-epdp-team/.

Активные участники пленарных заседаний Группы по EPDP: (LC – работал в Юридическом комитете)

Тип участника/принадлежность/имя	SOI	Дата начала	Участие в совещаниях %	Роль
Текущий участник			87,9%	
Член				
Консультативный комитет At-Large			97,7%	
Алан Гринберг (Alan Greenberg)	SOI	03.04.2019	97,7%	
Хадия Эль-Миньяви (Hadia El-Miniawi)	SOI	03.04.2019	97,7%	LC
Группа интересов коммерческих пользователей			94,8%	
Марджи Милам (Margie Milam)	SOI	03.04.2019	95,4%	LC
Марк Сванкарек (Mark Svancarek)	SOI	03.04.2019	94,3%	
Совет GNSO			98,3%	
Рафик Даммак (Rafik Dammak)	SOI	03.04.2019	98,3%	Председатель
Правительственный консультативный комитет			93,6%	
Кристофер Льюис-Эванс (Christopher Lewis-Evans)	SOI	15.05.2019	96,6%	
Георгиос Целентис (Georgios Tselentis)	SOI	03.04.2019	88,5%	
Лорин Каппин (Laureen Kappin)	SOI	21.10.2019	96,1%	LC
Правление ICANN			84,6%	
Бекки Берр (Becky Burr)	SOI	09.09.2019	93,5%	LC
Крис Дисспейн (Chris Disspain)	SOI	03.04.2019	78,2%	
Группа интересов по вопросам интеллектуальной собственности			91,0%	
Брайан Кинг (Brian King)	SOI	04.08.2019	88,5%	LC
Франк Журно (Franck Journoud)	SOI	12.01.2019	95,7%	
Интернет-корпорация по присвоению имен и номеров (ICANN)			95,9%	
Дэниэл Халлоран (Daniel Halloran)	-	03.04.2019	94,3%	
Элиза Агопян (Eleeza Agopian)	-	06.12.2019	98,4%	
Группа интересов интернет-провайдеров и провайдеров связи			65,5%	
Фиона Асонга (Fiona Asonga)	SOI	03.04.2019	44,8%	
Томас Рикерт (Thomas Rickert)	SOI	03.04.2019	86,2%	LC
Группа некоммерческих заинтересованных сторон			78,9%	
Амр Элсадр (Amr Elsadr)	SOI	03.04.2019	67,8%	
Йохан (Юлф) Хельсингиус (Johan (Julf) Helsingius)	SOI	03.04.2019	75,9%	
Милтон Мюллер (Milton Mueller)	SOI	03.04.2019	81,4%	
Стефан Филипович (Stefan Filipovic)	SOI	21.05.2019	84,5%	
Стефани Перрен (Stephanie Perrin)	SOI	03.04.2019	86,2%	LC
<вакантно>	-			

Группа заинтересованных сторон-регистраторов			85,0%	
Джеймс Блейдел (James Bladel)	SOI	03.04.2019	76,7%	
Мэтт Серлин (Matt Serlin)	SOI	03.04.2019	86,2%	
Фолькер Грейман (Volker Greimann)	SOI	16.04.2019	92,0%	LC
Группа заинтересованных сторон-регистратур			90,0%	
Алан Вудс (Alan Woods)	SOI	03.04.2019	90,8%	
Марк Андерсон (Marc Anderson)	SOI	03.04.2019	95,4%	
Мэтью Кроссмэн (Matthew Crossman)	SOI	03.04.2019	83,1%	LC
Консультативный комитет по безопасности и стабильности			92,1%	
Бен Батлер (Ben Butler)	SOI	03.04.2019	93,1%	
Тара Уэйлен (Tara Whalen)	SOI	15.05.2019	90,9%	LC

Активные участники-дублеры пленарных заседаний Группы по EPDP:

Тип участника/принадлежность/имя	SOI	Дата начала	Участие в совещаниях %	Роль
Дублер				
Консультативный комитет At-Large				
Бастиан Гослингс (Bastiaan Goslings)	SOI	03.04.2019	50,0%	
Холли Рэйчи (Holly Raiche)	SOI	03.04.2019	33,3%	
Группа интересов коммерческих пользователей				
Стив Дельбьянко (Steve DelBianco)	SOI	03.04.2019	100,0%	
Правительственный консультативный комитет				
Ольга Кавалли (Olga Cavalli)	SOI	22.05.2019	95,6%	
Рахул Госейн (Rahul Gosain)	SOI	03.04.2019	75,0%	
Райан Кэрролл (Ryan Carroll)	SOI	18.12.2019	100,0%	
Группа интересов интернет-провайдеров и провайдеров связи				
Суман Лал Прадхан (Suman Lal Pradhan)	SOI	03.04.2019	33,3%	
Группа некоммерческих заинтересованных сторон				
Дэвид Кейк (David Cake)	SOI	03.04.2019	90,0%	
Татьяна Тропина	SOI	03.04.2019	77,8%	LC
Йори Карр-Кирос (Yawri Carr Quirós)	SOI	17.02.2020	100,0%	
Группа заинтересованных сторон-регистраторов				
Оуэн Смигельски (Owen Smigelski)	SOI	16.04.2019	100%	
Сара Уайлд (Sarah Wyld)	SOI	03.04.2019	98,7%	
Тео Гёртс (Theo Geurts)	SOI	03.04.2019	80,0%	
Группа заинтересованных сторон-регистратур				
Арно Виттерсгейм (Arnaud Wittersheim)	SOI	03.04.2019	80,0%	
Бет Бейкон (Beth Bacon)	SOI	22.04.2019	95,7%	
Шон Басери (Sean Baseri)	SOI	06.11.2019	100,0%	
Консультативный комитет по безопасности и стабильности				
Грег Аарон (Greg Aaron)	SOI	05.10.2019	77,8%	
Род Расмуссен (Rod Rasmussen)	SOI	03.04.2019	25,0%	

Активная поддержка пленарных заседаний Группы по EPDP со стороны персонала:

Тип участника/принадлежность/имя	SOI	Дата начала	Участие в совещаниях %	Роль
Персонал поддержки				
ICANN (Интернет-корпорация по присвоению имен и номеров)				
Кейтлин Туберген (Kaitlin Tubergen)		03.04.2019		LC
Марика Конингс (Marika Konings)		03.04.2019		
Берри Кобб (Berry Cobb)		03.04.2019		LC
Эми Бивенс (Amy Bivens)		03.06.2019		LC
Терри Эгню (Terri Agnew)		03.04.2019		
Андреа Гландон (Andrea Glandon)		03.04.2019		
Джули Бисланд (Julie Bisland)		20.06.2019		
Мишель ДеСмайтер (Michelle DeSmyter)		20.06.2019		
Натали Перегрин (Nathalie Peregrine)		03.04.2019		

Бывшие участники пленарных заседаний Группы по EPDP:

Тип участника/принадлежность/имя	SOI	Дата начала	Участие в совещаниях %	Роль	Дата ухода
Бывший участник	-				
Член	-				
Совет GNSO	-				
Янис Карклинс (Janis Karklins)	SOI	03.04.2019	97,6%	Председатель	03.07.2020
Правительственный консультативный комитет	-				
Ашли Хайнеман (Ashley Heineman)	SOI	03.04.2019	75,7%		21.10.2019
Правление ICANN	-				
Леон Фелипе Санчес Амбиа (Leon Felipe Sanchez Ambia)	SOI	03.04.2019	88,5%	LC	09.09.2019
Группа интересов по вопросам интеллектуальной собственности	-				
Алекс Дикон (Alex Deacon)	SOI	03.04.2019	87,5%		01.12.2019
Интернет-корпорация по присвоению имен и номеров (ICANN)	-				
Дай-Транг Нгуен (Dai-Trang Nguyen)	-	03.04.2019	88,9%	LC	10.04.2019
Группа некоммерческих заинтересованных сторон	-				
Эйден Фабьен Ферделин (Ayden Fabien Férdeline)	SOI	03.04.2019	73,5%		27.01.2020
Фарзанех Бадий (Farzaneh Badiei)	SOI	03.04.2019	69,2%		27.01.2020
Группа заинтересованных сторон-регистратур	-				
Кристина Розетт (Kristina Rosette)	SOI	22.04.2019	97,6%		07.08.2019
Дублер	-				
Группа интересов по вопросам интеллектуальной собственности	-				
Дженнифер Гор (Jennifer Gore)	SOI	03.04.2019	97,6%		13.02.2020

Подробные сведения об участии в заседаниях находятся здесь: https://community.icann.org/x/4opHBQ.

Архивы электронной почты Группы по EPDP находятся здесь: https://mm.icann.org/pipermail/gnso-epdp-team/.

Приложение D. Обозначения консенсуса

Ниже приводится обозначение председателем уровня консенсуса по каждой рекомендации в итоговом отчете Группы по EPDP. Эти обозначения были сделаны в соответствии с процессом, изложенным здесь, и в соответствии с разделом 3.6 «Стандартная методика принятия решений» в Руководстве для Рабочих групп GNSO, а также в соответствии с уставом Группы по EPDP.

№ рекомендации		Обозначение, предложенное председателем	Группы, не поддерживающие рекомендацию или ее часть
№ 1	Аккредитация	Полный консенсус	
№ 2	Аккредитация правительственных организаций	Полный консенсус	
№ 3	Критерии и содержание запросов	Полный консенсус	
№ 4	Подтверждение получения	Полный консенсус	
№ 5	Требования к ответам	Значительная поддержка при наличии существенной оппозиции	GAC (точность) IPC BC
№ 6	Уровни приоритета	Расхождение во мнениях	GAC (не поддерживает 6.2) BC (не поддерживает 6.2) IPC (не поддерживает 6.2) ALAC (не поддерживает 6.2) SSAC
№ 7	Цели подателя запроса	Консенсус	NCSG (при условии удаления сноски)
№ 8	Авторизация сторон, связанных договорными обязательствами	Значительная поддержка при наличии существенной оппозиции	GAC (точность и возражение против 8.17) IPC BC
№ 9	Автоматизация обработки запросов в SSAD	Значительная поддержка при наличии существенной оппозиции	IPC BC ALAC
№ 10	Определение различных SLA для сроков ответа в SSAD	Значительная поддержка при наличии существенной оппозиции	RrSG (не поддерживает SLA для срочных запросов) SSAC IPC BC

№ 11	Условия и положения SSAD	Полный консенсус	
№ 12	Требования к раскрытию данных	Значительная поддержка при наличии существенной оппозиции	GAC (точность) SSAC
№ 13	Политика запросов	Полный консенсус	
№ 14	Финансовая устойчивость	Расхождение во мнениях	ALAC GAC SSAC IPC BC
№ 15	Ведение журналов	Полный консенсус	
№ 16	Аудиторские проверки	Полный консенсус	
№ 17	Требования к отчетности	Полный консенсус	
№ 18	Анализ реализации рекомендаций по политике в отношении SSAD с помощью Постоянного комитета GNSO	Значительная поддержка при наличии существенной оппозиции	ALAC BC IPC GAC
№ 19	Отображение информации об аффилированных провайдерах услуг сохранения конфиденциальности и регистрации через доверенных лиц	Полный консенсус	
№ 20	Поле «город»	Консенсус	NCSG
№ 21	Хранение данных	Полный консенсус	
№ 22	Цель № 2	Консенсус	NCSG

Приложение E. Заявления меньшинства

Консультативный комитет At-Large (ALAC)
Группа интересов коммерческих пользователей (BC) / Группа интересов по вопросам интеллектуальной собственности (IPC)
Правительственный консультативный комитет (GAC)
Группа некоммерческих заинтересованных сторон (NCSG)
Группа заинтересованных сторон-регистраторов (RrSG)
Группа заинтересованных сторон-регистратур (RySG)
Консультативный комитет по безопасности и стабильности (SSAC)

RU

AL-ALAC-ST-0720-04-01-EN
ОРИГИНАЛ: Английский язык
ДАТА: 29 июля 2020 года
СТАТУС: Ратифицировано

КОНСУЛЬТАТИВНЫЙ КОМИТЕТ AT-LARGE

Заявление ALAC по ускоренному процессу формирования политики (EPDP)

Заявление ALAC представлено для включения в Итоговый отчет по 2-й фазе ускоренного процесса формирования политики (EPDP) в области Временной спецификации для регистрационных данных в gTLD

ALAC делает следующее заявление в рамках своего участия в EPDP:

1. ALAC считает, что EPDP ДОЛЖЕН стать успешным, и будет работать в этом направлении.
2. Мы организуем структуру поддержки, чтобы гарантировать, что предлагаемое здесь будет понято нашим сообществом, которое предоставит комментарии и поддержку.
3. ALAC считает, что индивидуальные владельцы доменов являются пользователями, и мы регулярно работали от их имени (как в PDP, который мы инициировали для защиты прав владельцев доменов после истечения срока регистрации их доменов); если потребности владельцев доменов отличаются от потребностей 4 миллиардов пользователей интернета, которые не являются владельцами доменов, потребности последних имеют приоритет. Мы считаем, что GDPR и EPDP представляют собой именно такую ситуацию.
4. Хотя некоторые пользователи интернета обращаются к WHOIS и не смогут это сделать в некоторых случаях в будущем, наша главная забота — это доступ тех третьих сторон, которые стремятся сделать интернет безопасным местом для пользователей, а это означает, что правоохранительные органы, исследователи в сфере кибербезопасности, те, кто борется с мошенническим использованием доменных имен, и другие, которые помогают защитить пользователей от фишинга, вредоносного ПО, спама, мошенничества, DDoS-атак и так далее, могут работать с минимальным ограничением доступа к данным WHOIS. Конечно, с учетом ограничений GDPR.

Мы усердно трудились, чтобы поддержать процесс EPDP, и работаем от имени почти 5 миллиардов интернет-пользователей.

Целью фазы 2 EPDP была разработка того, что сейчас называется Системой обеспечения стандартизованного доступа к закрытым регистрационным данным

и их раскрытия (SSAD), а также решение ряда проблем, которые не были решены на фазе 1 EPDP.

Был проделан огромный объем работы, но ALAC считает, что после развертывания SSAD вероятность ее соответствия целям, поставленным сообществами, усилия которых мы поддерживаем, будет низкой. Этим сообществам нужен доступ к конкретным точным, пригодным для использования закрытым данным, и такой доступ должен быть своевременным и предсказуемым.

Ключевые методы достижения этого включают следующее:

- Не расширять сферу действия законодательства о конфиденциальности. Скрывать только данные, защищенные такими законами.
- Обеспечить, чтобы данные были точны, а контактная информация была пригодна для использования — это единственная причина наличия контактной информации.
- Насколько это возможно и законно, обрабатывать запросы в автоматическом режиме, что приводит к быстрым ответам (почти мгновенным, когда это возможно).

К сожалению, в итоговом отчете нет уверенности по этим вопросам.

А именно:

- На фазе 1 разрешено скрывать информацию как о юридических лицах (компаниях), так и о физических лицах (людях), и большинство регистраторов и регистратур полностью вымарывают данные. Они также скрывают данные вне зависимости от географического положения.
- Предполагалось, что на фазе 2 будет полностью решен вопрос о разделении юридических и физических лиц, но, несмотря на некоторое обсуждение, этот вопрос передается в Совет GNSO для возможного решения в будущем.
- GDPR требует, чтобы данные были точными для целей, в которых они обрабатываются. В случае данных RDS необходимо знать, кто является владельцем домена, и облегчить контакт. Исследования достоверности данных WHOIS показали, что в период, когда информация была общедоступной, она была крайне неточной. На фазе 2 предполагалось полностью обсудить вопрос точности в отношении теперь скрытых данных. Это не было сделано. Совет GNSO дал Группе по PDP указание не затрагивать эту тему, и Совет

GNSO рассмотрит вопрос о ее проработке не определенным пока образом.

- В настоящее время связь с владельцами доменов осуществляется с помощью методов (в основном веб-форм), которые, как показали исследования, неэффективны и не позволяют отправителю узнать о том, было ли сообщение доставлено владельцу домена. Дальнейшее обсуждение передано в Совет GNSO для возможного рассмотрения когда-нибудь в будущем.
- Есть несколько примеров использования, когда SSAD будет реагировать автоматически. Намерение состояло в том, что по мере развития законодательства, правовой практики и договорных вопросов механизм «развития» позволит распространить автоматизированную обработку на более широкий спектр примеров использования. Рекомендуемый механизм развития — это Постоянный комитет (SC) GNSO, который требует, чтобы новые примеры использования утверждались не только сторонами, связанными договорными обязательствами (которые могут быть привлечены к ответственности за невыполнение должным образом), но и Советом GNSO. SC может рекомендовать как чистую реализацию (для перехода к реализации требуется одобрение Совета GNSO), так и политику (для применения которой потребуется вначале осуществить процесс разработки политики GNSO, такой как PDP). Неясно, будут ли новые рекомендации по примерам использования решений SSAD рассматриваться как реализация, или потребуется организовать новый PDP (или аналог), чтобы фактически разрешить такую автоматизацию (потенциально добавляя годы, чтобы разрешить новые примеры использования).

  ALAC, наряду с несколькими другими группами, принял текущую модель SSAD, несмотря на серьезные оговорки, поскольку мы были уверены, что механизм развития позволит вносить изменения легко и своевременно. Такие изменения не были гарантированы из-за юридических проблем и вопросов ответственности, но они были возможны. Основываясь на том, что сейчас известно о механизме развития, и на отсутствии ясности в отношении того, как он будет работать и как его рекомендации будут рассматриваться Советом GNSO, ALAC, безусловно, никогда не согласился бы с текущей моделью SSAD.

Более того, хотя рекомендация Постоянного комитета по умолчанию требует стандартного большинства голосов Совета GNSO, есть вероятность того, что это можно будет изменить и ввести требование о необходимости квалифицированного большинства[48].

- Финансовая модель проблематична. На первый взгляд может показаться разумным, чтобы пользователи SSAD несли значительную часть эксплуатационных расходов, но при попытке добиться этого могут быть установлены настолько высокие цены, что они начнут препятствовать использованию. Это не только приведет к невыполнению поставленных финансовых целей, но и сведет на нет все усилия. Чтобы SSAD действительно можно было использовать, необходима гибкость в ценообразовании. В этом отношении пока неясно, в каком объеме может потребоваться субсидирование службы со стороны ICANN.

Все эти проблемы связаны с вопросами, которые Группе по EPDP было поручено не рассматривать, либо она решила не заниматься этим, либо формулировка рекомендации оставлена достаточно расплывчатой, чтобы не обеспечивать какой-либо уровень уверенности в результатах.

Все эти вопросы МОГУТ быть надлежащим образом решены Советом GNSO при обсуждении этого итогового отчета.

Соответственно, ALAC поддерживает этот отчет С ОПРЕДЕЛЕННЫМИ УСЛОВИЯМИ, в зависимости от действий Совета GNSO, указанных ниже.

Если эти результаты не могут быть достигнуты, ALAC считает, что этот отчет приведет к многолетнему внедрению и созданию системы, которая по сути станет раздутой, чрезмерно сложной и очень дорогой системой учета жалоб. Таким образом, итоговый отчет в целом, за исключением рекомендаций № 19–22, не получил нашей поддержки[49].

Результаты Совета GNSO, необходимые ALAC для поддержки итогового отчета EPDP:

1. Совет GNSO соглашается, что любая рекомендация Постоянного комитета по развитию по дополнительным вариантам использования решений SSAD (которые полностью соответствуют рекомендации № 9.3 политики EPDP) будет рассматриваться как реализация и не потребует дальнейшего обсуждения политики.

[48] Квалифицированное большинство голосов позволяет одной группе заинтересованных сторон и еще одному члену палаты наложить вето на любое действие GNSO.

[49] Настоящим поясняется следующее: если условия не будут выполнены, ALAC по-прежнему будет поддерживать рекомендации № 19-22, но не остальную часть отчета.

2. Юридические и физические лица, точность, система учета достоверности данных WHOIS и анонимный контактный адрес электронной почты будут всесторонне рассмотрены при полном участии во всех аспектах обсуждений консультативных комитетов ICANN, которые пожелают участвовать. Если эти вопросы считаются политикой, они должны решаться группой, уполномоченной давать рекомендации по политике, во главе с квалифицированным председателем, у которого нет конфликта интересов. GAC, ALAC и SSAC должны участвовать в определении полномочий или уставов таких групп. Срок завершения всех работ — не позднее апреля 2021 года.
3. Совет GNSO согласен с тем, что для ратификации рекомендаций Постоянного комитета по развитию потребуется простое большинство голосов в GNSO, как это в настоящее время предусмотрено в Руководстве по политике GNSO.
4. Совет GNSO признает, что в обсуждениях при установлении цен на использование SSAD должны участвовать будущие потенциальные пользователи SSAD и необходимо учитывать не только возмещение затрат, но и фактическую способность и готовность пользователей SSAD платить устанавливаемые цены.

Единогласно одобрено ALAC, 29 июля 2020 года
Представлено Аланом Гринбергом от имени ALAC

Дополнение к заявлению меньшинства ALAC по итоговому отчету фазы 2 EPDP

Члены консультативного комитета At-Large (ALAC) благодарны за возможность представить это дополнение к заявлению, которое было подано 29 июля 2020 года.

ALAC вместе с Группой по EPDP теперь имел возможность просмотреть и обсудить заявления, представленные BC/IPC, GAC и SSAC, а также заявления, представленные другими группами, входящими в состав EPDP.

Хотя ALAC, BC, IPC, GAC и SSAC использовали несколько разные подходы к изложению своих позиций в отношении отчета, ALAC в целом согласен с позициями, изложенными в заявлениях GAC, SSAC и BC/IPC. В частности, ALAC ценит глубокий и содержательный анализ, предоставленный GAC, SSAC и BC/IPC.

ALAC непросто выражать несогласие с итогами напряженных дебатов, длившихся более года. Чтобы было ясно, это не та ситуация, как предполагалось, когда мы не согласны, потому что «не добились своего». Если не решить проблемы, которые, по нашему мнению, критически важны для успеха SSAD, в результате получится система, которая не будет удовлетворять потребности пользователей SSAD, с небольшими возможностями для значительного исправления этих проблем

в будущем. Мы надеемся, что GNSO и, если уместно, Правление учтут это по мере продвижения процесса.

Ратифицировано ALAC 24 августа 2020 года.

Заявление об особом мнении Группы интересов коммерческих пользователей (BC) и Группы интересов по вопросам интеллектуальной собственности (IPC) относительно итогового отчета по фазе 2 EPDP

Итоговый отчет по фазе 2 EPDP не позволяет создать систему стандартизованного доступа, которая удовлетворяла бы потребности ее пользователей. Соответственно, Группа интересов коммерческих пользователей (BC) и Группа интересов по вопросам интеллектуальной собственности (IPC) вынуждены заявить о своем несогласии.

Как отмечалось в нашем заявлении по итоговому отчету по фазе 1 EPDP, BC и IPC являются стойкими сторонниками модели ICANN, основанной на консенсусе и принципе «снизу-вверх» с участием многих заинтересованных сторон, как видно из нашего добросовестного и активного участия в EPDP. Фаза 2 EPDP была направлена на создание стандартизованной системы, преследующей две цели: защита персональных данных владельцев доменов и предоставление пользователям последовательного, своевременного и предсказуемого доступа к данным владельцев доменов, когда пользователям необходимо обрабатывать эти данные на законных основаниях в своих легитимных целях. Поскольку в итоговом отчете по фазе 2 это не сделано, итоговый отчет по фазе 2 неприемлем.

Общие опасения

IPC и BC поддерживают защиту конфиденциальности персональных данных, а закон о конфиденциальности стремится найти баланс между правом личности на неприкосновенность частной жизни и другими законными интересами. К сожалению, в итоговом отчете по фазе 2 этот баланс не соблюдается. Это наносит ущерб тем, кто защищает свои основополагающие права, а также тем, кто действует в общественных или других законных интересах. Интересы членов BC включают обеспечение доверия пользователей к онлайн-коммуникациям и деловому взаимодействию (например, в соответствии с Директивой ЕС по NIS). Интересы членов IPC включают защиту потребителей от фишинга, опасной контрафактной продукции и другого мошенничества, как это предусмотрено в статье 38 Хартии ЕС по правам человека, а также защиту интеллектуальной собственности, как это предусмотрено в разделе 2 статьи 17 Хартии ЕС по правам человека.

IPC и BC отмечают, что в итоговом отчете по фазе 2 не учтены некоторые проблемы, поднятые Европейской комиссией и бельгийским органом по защите данных (DPA), а также собственными консультативными комитетами ICANN: Правительственным консультативным комитетом (GAC), представляющим интересы правоохранительных органов и органов защиты потребителей, Консультативным комитетом At-Large (ALAC), представляющим интересы конечных пользователей интернета, и Консультативным комитетом по

безопасности и стабильности (SSAC), отвечающим за консультирование Правления ICANN по вопросам, связанным с безопасностью и целостностью систем присвоения имен и распределения адресов в интернете.

Обеспокоенность, разделяемая Европейской комиссией и бельгийским DPA

Европейская комиссия[50] предлагала *«ICANN и сообществу разработать единую модель доступа, которая охватывает все регистратуры и всех регистраторов и обеспечивает наличие стабильного, предсказуемого и реалистичного способа получения доступа к закрытым регистрационным данным gTLD для пользователей, у которых есть законный интерес или другое законное основание, предусмотренное в Общем регламенте по защите данных (GDPR)».* Европейская комиссия заявила, что считает это «*жизненно важным и срочным*» и призвала ICANN «*разработать и внедрить прагматичную и работоспособную модель доступа в кратчайшие сроки…*». Бельгийский DPA, который является надзорным органом корпорации ICANN в связи с местонахождением ее офиса в Бельгии, назвал централизованную модель «*более качественным и здравым решением с точки зрения обеспечения защищенности субъектов данных*».[51] К сожалению, в итоговом отчете по фазе 2 вообще отсутствует способ доступа, не говоря уже о способе, который можно было бы описать как «*стабильный, предсказуемый и работоспособный*». Напротив, в итоговом отчете по фазе 2 просто предлагается центральное место для подачи запросов. Тем самым отклоняются указания бельгийского DPA в пользу того, чтобы оставить решение о раскрытии данных на усмотрение более двух тысяч отдельных сторон, связанных договорными обязательствами, ни одна из которых не обязана в соответствии с контрактами или политикой ICANN нанимать юриста, сотрудника по защите данных или специалиста по конфиденциальности.

Обеспокоенность BC и IPC, которую разделяет GAC

Мы также разделяем обеспокоенность GAC по поводу неспособности Группы по EPDP решить вопросы точности данных и различия между юридическими и физическими лицами. В своем письме от 22 июня Совету GNSO[52] GAC отметил, что «*Эти вопросы имеют решающее значение для общественных интересов. Если не решить эти проблемы в рамках текущего EPDP, возникает риск создания неполной системы, в которой не будет ключевых возможностей, способствующих общественной безопасности. Более того, неспособность решить эти важные вопросы ставит под сомнение легитимность и эффективность процесса разработки политики GNSO для решения вопросов,*

[50] См. https://www.icann.org/en/system/files/correspondence/odonohue-to-marby-03may19-en.pdf
[51] См. https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority
[52] См. https://gac.icann.org/advice/correspondence/outgoing/GAC%20Chair%20letter%20to%20GNSO%20Council%20Chair%20-%20Next%20Steps%20on%20Key%20Policy%20Issues%20not%20Addressed%20in%20EPDP%20Phase%202.pdf

которые представляют важность для заинтересованных сторон, не входящих в GNSO, и общественных интересов.» К сожалению, на фазе 2 просьбы GAC были проигнорированы. Несмотря на то, что GDPR требует точности данных, Совет GNSO исключил точность из круга задач фазы 2 EPDP, а в итоговом отчете по фазе 2 не была учтена необходимость проводить различие между юридическими и физическими лицами, являющимися владельцами доменов.

Обеспокоенность BC и IPC, которую разделяют SSAC и ALAC

Комментарий SSAC к первоначальному отчету фазы 1 EPDP (SSAC 111[53]) содержал многочисленные опасения, что рекомендации «*далеки от того, что, по мнению SSAC, необходимо и можно сделать для решения проблем безопасности и стабильности в рамках полномочий ICANN*». Аналогичным образом, ALAC, среди прочего, в своем Заявлении от 5 мая 2020 года относительно дополнения к первоначальному отчету[54] также выразил обеспокоенность по поводу неспособности решить проблемы, связанные с различием между юридическими и физическими лицами, являющимися владельцами доменов, и точностью.

Существенные недочеты итогового отчета по фазе 2 EPDP

В дополнение к опасениям, ранее высказанным GAC, ALAC и SSAC, следующие недостатки отчета по фазе 2 вызывают несогласие BC и IPC.

- ***Отсутствие централизованного раскрытия информации и недостаточные механизмы развития***. После фазы 1 мы рассчитывали на разработку политики, поддерживающей централизованное принятие решений. Неэффективность и непоследовательность децентрализованного принятия решений очевидны: более высокие затраты для сторон, связанных договорными обязательствами, более медленная обработка запросов о раскрытии данных и большая вероятность споров между подателями запросов и раскрывающими данные сторонами, поскольку каждая сторона, связанная договорными обязательствами, применяет свое собственное субъективное суждение к каждому запросу.

  Тем не менее, в интересах компромисса мы согласились рассмотреть (но не принять) предложенную *гибридную модель*, где решения о раскрытии данных первоначально будут в основном приниматься децентрализованно и вручную, но затем будет совершен переход к автоматизированной и централизованной обработке на основе опыта, полученного во время внедрения SSAD, и повышения правовой ясности в отношении интерпретации требований GDPR.

[53] См. https://www.icann.org/en/system/files/files/sac-111-en.pdf
[54] См. https://atlarge.icann.org/advice_statements/13775

Мы ожидали, что со временем система с соответствующими механизмами защиты будет автоматически предоставлять запрошенные данные владельца домена для установленных легитимных целей аккредитованным подателям запросов на их собственных законных основаниях. Например, аккредитованные податели запросов с разумными доказательствами торговли контрафактной продукцией или нарушения авторских прав, заявленных под страхом наказания за лжесвидетельство, должны быстро и предсказуемо получить данные о владельцах соответствующих доменных имен. Ясность, последовательность и масштабируемость такой системы значительно повысили бы доверие и подотчетность в DNS, поскольку доступ к этим данным всегда был, но не предусмотрен в итоговом отчете по фазе 2.

Отчет по фазе 2 не позволяет ICANN развиваться до своей естественной роли централизованного органа, принимающего решения. Вместо этого он дает сторонам, связанным договорными обязательствами, неоправданные возможности толковать свои обязательства в соответствии с GDPR и своими контрактами с ICANN без каких-либо требований в отношении разумности, единообразия или других механизмов защиты. Он также не может обеспечить создание адекватного механизма, обеспечивающего централизацию и автоматизацию в будущем. При этом он навсегда фиксирует неэффективность децентрализованного принятия решений, например, приводящую к необоснованно длительным срокам в SLA даже для срочных запросов, связанных с неминуемыми угрозами жизни или критически важной инфраструктурой. (Рекомендации № 9 и № 18)

- ***Отсутствие дифференцированного подхода к физическим и юридическим лицам***. Предоставляя сторонам, связанным договорными обязательствами, единоличное право определять, следует ли проводить различие между физическими и юридическими лицами, отчет по фазе 2 не обеспечивает ясность в отношении доступа к данным владельцев доменов для *юридических лиц*, на которых не распространяется действие GDPR. Группа по EPDP запросила и получила юридические рекомендации от компании Bird & Bird, внешнего юрисконсульта, которого Группа по EPDP привлекла для получения рекомендаций по обязательствам GDPR, по вопросу разграничения юридических и физических лиц, являющихся владельцами доменов. Но обсуждение этих рекомендаций не состоялось, несмотря на возражения IPC, BC, GAC, SSAC и ALAC. GDPR не требует постоянного массового сокрытия контактных данных юридических лиц[55],

[55] В комментариях, представленных Afnic относительно дополнения к отчету по фазе 2, поддерживается эта точка зрения. «*Мы хотели бы поделиться озабоченностью по поводу подхода, предлагающего не проводить различие между зарегистрированными доменными именами юридических и физических лиц. Как уже отмечалось многими авторами комментариев, мы считаем это чрезмерным применением GDPR. Несмотря на то, что GDPR не защищает данные, относящиеся к юридическим лицам, мы хотели бы напомнить ICANN, что в ее письме от 11 декабря 2017 года, WP29*

и это подрывает доверие, подотчетность и транспарентность в DNS. Таким образом, это представляет собой неприемлемый недостаток EPDP. (Рекомендация № 8)

- ***Неспособность решить проблему точности данных***. В отчете по фазе 2 не рассматривается фундаментальная проблема точности данных владельцев доменов, как было согласовано в рамках EPDP на фазе 1, несмотря на то, что на сегодняшний день существуют адекватные инструменты для проверки точности данных владельцев доменов. Неточность данных WHOIS остается проблемой уже более 20 лет. Группа по EPDP не последовала юридическому совету, который она запросила в отношении интерпретации требований к точности в рамках GDPR. Группа по EPDP также не последовала совету Европейской комиссии, которая подтвердила, что точность данных отвечает интересам не только субъекта данных. Явно ложные данные не защищены законами о конфиденциальности данных, и сохранение массового сокрытия ложных или фиктивных данных владельца домена в DNS представляет собой еще один недочет EPDP, который еще больше подрывает доверие, подотчетность и транспарентность в DNS. (Заключение 2)

- ***Неадекватная правоприменительная политика***. В отчете по фазе 2 отсутствует какая-либо договорная подотчетность для сторон, связанных договорными обязательствами, по предоставлению данных в ответ на законные запросы. Как упоминалось выше, отчет по фазе 2 не может адекватно предоставить объективную основу и последовательную, предсказуемую и масштабируемую процедуру для надежного получения аккредитованными пользователями точных данных о владельце домена, когда есть законные основания и легитимные цели для запроса и использования данных, даже если бы такие данные и не должны были скрываться. Отчет по фазе 2 не позволяет ICANN обеспечивать соблюдение слабых рекомендаций, содержащихся в отчете. Децентрализованная SSAD не имеет особой ценности, если нет механизма, обеспечивающего соблюдение согласованной политики. К сожалению, в этом отчете рассматривается только соблюдение процедурных требований и он не позволяет отделу по контролю исполнения договорных обязательств ICANN рассматривать неправомерные отклонения законных запросов. Это подрывает и лишает легитимности всю политику. (Рекомендации № 5 и № 8)

Результатом является отчет по фазе 2, в котором рекомендуется система и политика, полностью не соответствующие заявленным и согласованным целям SSAD, включая потребности ее пользователей. В результате отчет по фазе 2 не может обеспечить доверие, безопасность и отказоустойчивость DNS.

При разработке этой политики важно, чтобы сообщество ICANN поддержало усилия по борьбе с растущим злоупотреблением доменными именами, которое угрожает безопасности, стабильности и отказоустойчивости DNS и экосистемы интернета в более широком смысле, включая безопасность ее конечных пользователей. Недавно компания Neustar (сторона, связанная договорными обязательствами), сообщила об общем росте интернет-трафика из-за пандемии COVID-19 и сопутствующих кибератак: «*Neustar ожидала увеличения числа атак, но мы наблюдаем резкое увеличение числа атак с использованием практически всех измеряемых нами показателей. Мы наблюдаем увеличение общего количества атак, а также их тяжести...*»[56] Помимо того, что она «*предотвратила возросшее более чем вдвое количество атак в 1-м квартале 2020 года по сравнению с 1-м кварталом 2019 года*», Neustar сообщила о «*росте объемов перехвата DNS, при котором настройки DNS меняются, чтобы перенаправить пользователя на сайт, который внешне может выглядеть таким же, но часто содержит вредоносное ПО, замаскированное под что-то полезное».*

Сведения об уровне консенсуса

IPC и BC напоминают Совету GNSO и Правлению ICANN, что итоговый отчет по фазе 2 EPDP определяет политику для единой **системы** (а именно SSAD). Хотя оценка уровня консенсуса осуществляется по каждой рекомендации отдельно, они по своей природе взаимосвязаны из-за их воздействия и влияния на SSAD в целом. Таким образом, результат оценки консенсуса следует рассматривать комплексно на уровне системы, а не строго в разрезе каждой рекомендации.

№ рекомендации	
№ 1 Аккредитация	За
№ 2 Аккредитация правительственных организаций	За
№ 3 Критерии и содержание запросов	За
№ 4 Подтверждение получения	За
№ 5 Требования к ответам	Против
№ 6 Уровни приоритета	Против
№ 7 Цели подателя запроса	За
№ 8 Авторизация сторон, связанных договорными обязательствами	Против
№ 9 Автоматизация обработки запросов в SSAD	Против
№ 10 Определение различных SLA для сроков ответа в SSAD	Против
№ 11 Условия и положения SSAD	За
№ 12 Требования к раскрытию данных	За
№ 13 Политика запросов	За
№ 14 Финансовая устойчивость	Против
№ 15 Ведение журналов	За
№ 16 Аудиторские проверки	За

[56] См. https://www.home.neustar/resources/whitepapers/covid-19-online-traffic-and-attack-data-report

№ 17 Требования к отчетности	За
№ 18 Анализ реализации рекомендаций по политике в отношении SSAD с помощью Постоянного комитета GNSO	Против
№ 19 Отображение информации об аффилированных провайдерах услуг сохранения конфиденциальности и регистрации через доверенных лиц	За
№ 20 Поле «город»	За
№ 21 Хранение данных	За
№ 22 Цель № 2	За

Кроме того, IPC и BC выступают против формулировок в следующих разделах, не являющихся рекомендациями:

- Разделы 1.2 и 2.3 (описание «не рассмотренных вопросов»). Мы не поддерживаем описание результатов по юридическим и физическим лицам.
- Раздел 3.1 (описание того, как мы пришли к «гибридной» модели). Наше согласие с переходом к гибридной модели было обусловлено возможностью переноса централизованных решений в CGM с течением времени с использованием механизма развития, который поддерживал бы это.
- Заключение — точность (стр. 60).

Оценка общей ценности для подателей запросов

Хотя Группа по EPDP на фазе 2 потратила много времени и усилий на анализ финансовой устойчивости самой SSAD, мы считаем, что не менее важно проанализировать затраты и выгоды с точки зрения пользователей (то есть пользователей системы, желающих получить данные о владельце домена). Это очень важно, учитывая, что политика фазы 2 требует, чтобы податели запросов оплачивали большую часть, если не все затраты на текущую эксплуатацию и обслуживание SSAD, и, таким образом, мы ожидаем, что размер сборов за аккредитацию и запросы, подлежащих уплате подателями запросов, будет значительным.

Кроме того, политика SSAD, как она определена в настоящее время, окажет существенное влияние, помимо прямых затрат, на тех, кто исторически полагался на данные WHOIS. Эти косвенные затраты связаны со следующим:

- **Несвоевременный ответ**: Из-за ранее описанных недочетов сроки ответа на запросы о раскрытии данных будут неприемлемо долгими, что повлияет на эффективность процессов, связанных с расследованием и противодействием злоупотреблениям и противозаконным действиям.

- **Неполнота**: Поскольку больше нет возможности выполнять так называемый «обратный поиск», теперь труднее идентифицировать все домены, связанные с событием или атакой.

- **Отсутствие привязки**: Блокировка обратного поиска препятствует возможности связать преступную деятельность или злоупотребления с владельцем домена (субъектом) в окне полноценного реагирования (если это вообще возможно). Податели запросов, особенно службы быстрого реагирования на кибератаки, при принятии контрмер или смягчении атак будут в большей степени полагаться на факторы близости, а не на привязку.

- **Неточность**: Нет никакой гарантии, что возвращенные данные будут точными, а также нет положений о том, чтобы независимые стороны проверяли точность регистрационных данных. Податели запросов обременены расходами на запросы о раскрытии данных без уверенности в полезности или ценности ответа.

- **Отсутствие сдерживания**: Невозможность своевременно составить полный список доменов, связанных с преступной или злонамеренной деятельностью, задерживает быстрое реагирование на кибератаки. Таким образом, атаки будут длиться намного дольше, чем раньше, когда целевым временем смягчения последствий был интервал от 1 до 4 часов. Определенные в настоящее время SLA, недостаточны для решения таких проблем, как фишинг, длящийся часы, а не дни, или атаки вредоносного ПО, которые наносят серьезный и прямой ущерб своим жертвам.

- **Непредсказуемость**: Децентрализованная и распределенная модель раскрытия данных приведет к непредсказуемой и ненадежной системе доступа и раскрытия. Это блокирует попытки подателей запросов получить данные у нескольких сторон, связанных договорными обязательствами, о большом количестве доменов, связанных с одним киберпреступлением или злоупотреблением.

Мы всегда признавали необходимость уплаты аккредитационных сборов за использование SSAD. Однако очевидно, что ценность и выгоды SSAD, как они определены в итоговом отчете по фазе 2, вовсе не оправдывают затрат (прямых и косвенных) на использование SSAD.

Заключение

Когда Правление ICANN в мае 2018 года приняло Временную спецификацию, оно отмечало, что «*решения Правления не окажут непосредственного влияния на безопасность, стабильность и отказоустойчивость DNS, поскольку это поможет сохранить службу WHOIS в максимально возможной степени,*

пока сообщество разрабатывает согласованную политику».[57] На конференции ICANN66 в Монреале в ноябре 2019 года Правление и генеральный директор ICANN подтвердили на открытом форуме важность масштабируемого доступа к данным владельцев доменов для обеспечения безопасности и защиты интернета и его пользователей. Результаты более чем двухлетней интенсивной работы Группы по EPDP представляют собой не что иное, как подтверждение статус-кво [до EPDP]: элементы данных WHOIS, необходимые для идентификации владельцев и пользователей доменных имен, в основном недоступны для физических и юридических лиц, которые служат законным общественным и частным интересам.

По указанным выше причинам наши утвержденные Правлением миссии и цели вынуждают нас не согласиться с набором рекомендаций по политике, изложенных в итоговом отчете по фазе 2.

Несмотря на благие намерения IPC и BC, эксперимент EPDP провалился. Он оказался неспособным решить чисто юридическую проблему, созданную GDPR. Регулирующим и законодательным органам следует учитывать, что модель с участием многих заинтересованных сторон ICANN не отвечает требованиям защиты потребителей, кибербезопасности и правоохранительных органов. Как следствие, существует потребность в четких нормативных указаниях для GDPR и в применении альтернативных правовых и нормативных подходов.

О группах BC и IPC

Миссия Группы интересов коммерческих пользователей (BC), утвержденная Правлением ICANN, заключается в «*обеспечении подотчетности и транспарентности ICANN при выполнении своих функций, а также того, чтобы ее позиции в области политики соответствовали развитию такого интернета, который... способствует укреплению доверия пользователей к онлайн-коммуникациям и деловому взаимодействию...*».

Целью Группы интересов по вопросам интеллектуальной собственности (IPC), утвержденной Правлением ICANN, является «*выражение взглядов и интересов владельцев интеллектуальной собственности во всем мире с особым упором на товарные знаки, авторские права и связанные с ними права на интеллектуальную собственность, их влияние и взаимодействие с системами доменных имен (DNS), а также отражение этих взглядов, в том числе взглядов меньшинства, в рекомендациях Совета GNSO Правлению ICANN*».

[57] См. https://www.icann.org/resources/board-material/resolutions-2018-05-17-en

Особое мнение Правительственного консультативного комитета в отношении итогового отчета по фазе 2 EPDP в области регистрационных данных gTLD

Примечание. *Консультативный комитет At-Large (ALAC), Группа интересов коммерческих пользователей (BC) и Группа интересов по вопросам интеллектуальной собственности (IPC) поддерживают мнения, выраженные в этом комментарии.*

Введение

GAC искренне ценит усилия всей Группы по EPDP, ее целеустремленных председателей и персонала ICANN из группы поддержки за последние 23 месяца и признает, что на разработку этих сложных и важных рекомендаций по политике в отношении доступа к регистрационным данным доменных имен и их раскрытия (ранее известной как WHOIS) было потрачено много времени и усилий.
Устав ICANN признает, что данные WHOIS необходимы для «законных нужд правоохранительных органов» и для «углубления доверия потребителей».[58]
GAC также неоднократно признавал эти важные цели, отмечая, что данные WHOIS используются для ряда законных действий, включая: оказание помощи правоохранительным органам в расследованиях; помощь предприятиям в борьбе с мошенничеством и неправомерным использованием интеллектуальной собственности, защита интересов общества и содействие доверию пользователей к интернету как надежному средству информации и коммуникации.[59]

Признавая эти важные цели, Временная спецификация ICANN для регистрационных данных в gTLD была направлена на «обеспечение непрерывной доступности WHOIS в максимально возможной степени при сохранении безопасности и стабильности системы уникальных идентификаторов интернета».[60] Итоговые рекомендации содержат полезные элементы, которые являются улучшением по сравнению с текущей Временной спецификацией, регулирующей доступ к регистрационным данным доменного имени. Тем не менее, GAC вынужден воздержаться от поддержки определенных рекомендаций, которые в их нынешней форме не обеспечивают надлежащего баланса между защитой прав лиц, предоставляющих данные регистратурам и регистраторам, и защитой общественности от вреда со стороны злоумышленников, стремящихся использовать систему доменных имен в своих интересах.[61] В этой связи GAC

[58] Устав ICANN, проверка службы каталогов регистрационных данных, §4.6(e).
[59] *См., например,* Коммюнике GAC по результатам заседаний на конференции в Абу-Даби, раздел VII.3, стр. 11, и Принципы GAC в отношении служб WHOIS (2007 год).
[60] *См. веб-страницу «Вопросы защиты персональных данных» на сайте ICANN*: https://www.icann.org/dataprotectionprivacy
[61] GAC (вместе с другими группами заинтересованных сторон) возражал против следующих рекомендаций: 5 — Требования к ответам; 6 — Уровни приоритета; 8 — Авторизация сторон, связанных договорными обязательствами; 14 — Финансовая устойчивость; 18 — Анализ реализации рекомендаций по политике в

подчеркивает, что система доменных имен является глобальным общедоступным ресурсом, который должен обслуживать потребности всех своих пользователей, включая потребителей, предприятия, владельцев доменов и правительства.

В настоящем заявлении меньшинства GAC комментирует проблемы общественной политики, связанные с тем, что итоговые рекомендации:

1) в настоящее время подразумевают не централизованную, а фрагментированную систему раскрытия данных;
2) в настоящее время не содержат обязательных для соблюдения стандартов пересмотра решений о раскрытии данных;
3) не уделяют достаточного внимания опасениям, связанным с защитой прав и доверия потребителей;
4) в настоящее время не содержат надежных механизмов дальнейшего развития системы стандартизованного доступа к данным и их раскрытия (SSAD) по мере роста правовой определенности;
5) могут привести к возникновению финансовых условий, чреватых тем, что система SSAD возложит несоразмерные затраты на своих пользователей, в том числе на тех, которые занимаются обнаружением и реагированием на угрозы в области кибербезопасности.

Кроме того, как подчеркивалось в нашем Комментарии GAC относительно дополнения к первоначальному отчету по фазе 2 EPDP, в итоговом отчете в настоящее время не рассматриваются некоторые ключевые проблемы (в первую очередь точность данных, сокрытие данных юридических лиц, не защищенных GDPR, и использование анонимных адресов электронной почты). Модель оставляет желать большего в том, что касается уточнения статуса и роли контролеров и сторон, ответственных за обработку данных. GAC просит Совет GNSO обеспечить незамедлительное рассмотрение этих важных вопросов в рамках этого EPDP в качестве следующей и заключительной фазы 3.

Фрагментированная система раскрытия данных

Хотя в итоговых рекомендациях описана централизованная система подачи запросов, отсутствует такая централизация в отношении раскрытия данных. Текущие рекомендации создают фрагментированную систему, которая может привести к неадекватному доступу к регистрационным данным и создать задержки при расследований правонарушений, нарушений в области интеллектуальной собственности и кибербезопасности. GAC предостерег от создания «раздробленной системы предоставления доступа, в которой могут применяться тысячи разных принципов политики, в зависимости от конкретного регистратора», отметив, что «отсутствие согласованной политики доступа к

отношении SSAD с помощью Постоянного комитета GNSO. *См.* «Сведения об уровне консенсуса» в Приложении D к итоговому отчету по фазе 2 EPDP.

закрытым данным вызывает задержки», которые могут препятствовать расследованиям и могут обеспечивать возможность потенциально вредоносного поведения, причиняющего вред общественности.[62] По мнению GAC, такой результат не соответствует ожиданиям GAC относительно «стабильных, предсказуемых и работающих механизмов доступа к закрытой информации WHOIS».[63] Примечательно, что бельгийский орган по защите данных признал потенциальные преимущества централизованной модели и прямо признал, что GDPR не запрещает автоматизацию различных функций в модели раскрытия данных. [64]

Тем не менее, рекомендации по раскрытию данных:

- почти полностью полагаются на индивидуальные оценки и решения более 2000 аккредитованных ICANN регистраторов;[65]
- недостаточно учитывают роль автоматизации и предусматривают только две категории автоматизированных ответов;[66] а также
- предусматривают недостаточные меры для создания надежных механизмов расширения категорий запросов, подходящих для автоматизированного раскрытия данных в ответ на будущие правовые рекомендации или даже изменения в применимом законодательстве о конфиденциальности.[67]

Нынешняя фрагментированная система раскрытия данных в сочетании с относительно неопределенной концепцией рассмотрения и подготовки рекомендаций по будущей централизации может препятствовать стабильности и предсказуемости SSAD.

Отсутствие обязательных для соблюдения стандартов пересмотра решений о раскрытии данных

GAC признает, что в соответствии с применимыми правилами защиты данных, включая GDPR, стороны, связанные договорными обязательствами, скорее всего, останутся ответственными за принятие решения о раскрытии регистрационных данных доменного имени и могут столкнуться с определенными рисками ответственности, связанными с этим решением. GAC понимает, что стороны, связанные договорными обязательствами, в связи с этим стремились сохранить контроль над решением о раскрытии регистрационных данных доменного имени.

[62] Коммюнике по результатам заседаний GAC в Барселоне (Раздел IV.2 «Прочие вопросы» — ссылка на Временную спецификацию, стр.6).
[63] Коммюнике по результатам заседаний GAC в Панаме, см. обоснование согласованной рекомендации GAC Правлению ICANN (раздел V.1, стр. 7)
[64] https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority
[65] Рекомендация (Рек.) 8
[66] Рек. 9.41 и 9.42
[67] Рек. 8.17 и 18

Тем не менее, GAC отмечает, что эти децентрализованные решения о раскрытии данных в значительной степени не подлежат оспариванию и принудительным мерам, в частности, через отдел по контролю исполнения договорных обязательств ICANN.[68]

Регистрационные данные важны для безопасности и стабильности DNS, и существует реальная обеспокоенность по поводу того, что стороны, связанные договорными обязательствами, могут случайно или намеренно неправильно взвесить общественные интересы для подателя запроса на получение таких данных. Генеральный директор ICANN недавно сообщил об этой обеспокоенности Европейскому совету по защите данных, указав, что «из-за отсутствия правовой определенности регистраторы, как контролеры, скорее всего, будут оценивать конфиденциальность и защиту данных в абсолютном выражении, не принимая во внимание другие права и законные интересы, чтобы избежать возможных санкций со стороны регулирующих органов или судебного решения против них».[69] Отказ в удовлетворении законных запросов о доступе к регистрационным данным доменного имени имеет реальные последствия. GAC отметил в своем Коммюнике по результатам заседаний в Барселоне следующее: опросы и исследования показали, что введение Временной спецификации в ответ на GDPR оказало негативное влияние на способность правоохранительных органов и специалистов по кибербезопасности расследовать преступления и бороться с ними, используя информацию, которая когда-то была общедоступной в системе WHOIS.[70]

Текущие рекомендации не предоставляют механизма для проверки решений о раскрытии данных. Предлагаемая на данном этапе система не включает роль отдела по контролю исполнения договорных обязательств ICANN в области рассмотрения существенных проблем, связанных с решениями о раскрытии данных. Вместо этого отдел по контролю исполнения договорных обязательств ICANN играет ограниченную роль в рассмотрении жалоб на несоблюдение *процедурных* требований или систематические злоупотребления.[71] В результате

---

68 Рек. 8, Рек. 5.3 и 5.4. ***См. также*** Письмо генерального директора ICANN от 22 мая 2020 года в Европейский совет по защите данных, https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-22may20-en.pdf.

69 *См.* Письмо генерального директора ICANN от 22 мая 2020 года в Европейский совет по защите данных, https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-22may20-en.pdf («Неопределенность в том, как обеспечить при доступе к данным баланс законных интересов с интересами субъекта данных, оставляет многое на субъективное усмотрение регистратора, как контролера, получающего запрос на доступ и принимающего решение о том, предоставить ли доступ к закрытым регистрационным данным gTLD или отказать в нем»).

70 *См.* также раздел 5.2.1 в Итоговом отчете 2-й группы по анализу служб каталогов регистрационных данных (3 августа 2019 года) и результаты совместного опроса, проведенного Антифишинговой рабочей группой и Рабочей группой по борьбе со злоупотреблениями и вредоносным ПО при передаче сообщений и использовании мобильной связи (18 октября 2018 года).

71 Рек. 5.3–5.5. Более того, руководство по реализации даже не требует от сторон, связанных договорными обязательствами, корректировать свой анализ решений о раскрытии «с учетом применимого прецедентного права, интерпретирующего GDPR, руководящих принципов, выпущенных EDPB, или

рекомендации по SSAD продвигают систему, в которой существует угроза стимулирования консервативного подхода к решениям о раскрытии данных для снижения рисков ответственности и которая не обеспечивает надлежащего анализа решений о раскрытии данных в рамках механизмов принудительного исполнения ICANN. Предоставление сторонам, связанными договорными обязательствами, полной свободы действий при рассмотрении требований о раскрытии данных может отрицательно сказаться на обязательстве обеспечивать постоянную возможность применения регистрационных данных доменных имен в качестве инструмента защиты прав и интересов общественности, органов, которым поручена защита общественности, а также Группы интересов коммерческих пользователей и Группы интересов по вопросам интеллектуальной собственности. GAC считает, что этот предлагаемый в настоящее время подход может препятствовать стабильности и предсказуемости SSAD.

Приоритет запросов, поднимающих проблемы защиты потребителей

GAC обеспокоен неадекватным приоритетом запросов, связанных с защитой потребителей (поднимающих проблемы, связанные с фишингом, вредоносным ПО и мошенничеством),[72] причиной которых является серьезная озабоченность общественности, зачастую требующая немедленных действий.[73] Текущие рекомендации помещают запросы, связанные с защитой потребителей, на самый низкий из трех уровней приоритета. Более того, соответствующие требования к уровню обслуживания, которые регламентируют время реагирования на запросы с приоритетом 3, предусматривают длительный срок ответа: в течение пяти дней в первые шесть месяцев внедрения, а затем срок ответа удваивается до 10 дней.[74] Неправильная расстановка приоритетов и длительное время реагирования могут привести к значительному ущербу, который быстро могут причинить мошенничество и кибератаки. GAC рекомендует присвоить запросам, связанным с защитой потребителей, уровень приоритета 2.

Даже если принять текущее назначение приоритета 3, предложенное действие рекомендации № 6 вызывает озабоченность. GAC приветствует тот факт, что рекомендация требует предоставить подателю запроса возможность помечать запросы, которые связаны с вопросами защиты потребителей («податели запросов ДОЛЖНЫ иметь возможность указать, что запрос о раскрытии данных

изменений GDPR или других применимых законов о конфиденциальности, которые могут появиться в будущем». *См.* Рек. 8.17. В Руководстве используется слово «СЛЕДУЕТ», а не «ДОЛЖЕН», и поэтому оно не подлежит принудительному исполнению (см. электронное письмо Группе по EPDP от 19 декабря 2019 года от представителей ICANN, обсуждающих возможность принудительного исполнения при использовании терминов «СЛЕДУЕТ» и «ДОЛЖЕН»).

72 GAC также отмечает, что предлагаемое определение запросов, связанных с защитой потребителей, представляется излишне ограничивающим, и просит интерпретировать заключенный в скобки текст как иллюстративный, а не исчерпывающий.

73 *См.* Комментарий SSAC к первоначальному отчету по фазе 2 ускоренного процесса формирования политики в области Временной спецификации для регистрационных данных в gTLD (SAC 111) на стр. 9–10.

74 Рек. 6.2 и Рек. 10.4 и 10.11.

касается защиты потребителей. . .»).[75] Однако эта рекомендация не содержит аналогичного обязательного требования для сторон, связанных договорными обязательствами, отдавать приоритет запросам, связанным с защитой потребителей, перед другими запросами с тем же уровнем приоритета. Вместо того чтобы использовать слово «ДОЛЖЕН», в рекомендациях говорится, что сторонам, связанным договорными обязательствами, «СЛЕДУЕТ» уделять первостепенное внимание этим запросам.[76] Однако отдел по контролю исполнения договорных обязательств ICANN прямо проинформировал Группу по EPDP о том, что использование слова «СЛЕДУЕТ» не влечет за собой появление обязательства, исполнимого в принудительном порядке[77]. Следовательно, данная рекомендация внутренне непоследовательна в том смысле, что она требует способности выявлять проблемы защиты потребителей, но не требует, чтобы стороны, связанные договорными обязательствами, принимали во внимание эту категорию. Обсуждения этой проблемы в Группе по EPDP показали, что указанная цель может быть достигнута просто с помощью механизма сортировки. Запросы, связанные с защитой потребителей, вызывают проблемы, которые влияют на общую безопасность DNS, и поэтому GAC рекомендует сделать эту расстановку приоритетов обязательной, а не разрешительной.

Надежные механизмы улучшения SSAD

SSAD, как и любая новая система, столкнется с проблемами при ее внедрении и применении, на которые потребуется своевременно реагировать. Механизмы могут требовать корректировки, требования со стороны лиц, запрашивающих данные, подвержены метаморфозам, и могут появиться новые и непредвиденные способы использования данных, особенно в сфере кибербезопасности. Соответственно, потенциал SSAD в области будущего улучшения, адаптации к новым препятствиям и реагирования на новые правовые рекомендации имеет решающее значение.

Что касается автоматизации, итоговая рекомендация по автоматизированному принятию решений о раскрытии данных требует автоматизации обработки любых категорий запросов, для которых автоматизация определена как «технически и коммерчески осуществимая и допустимая с юридической точки зрения».[78] Хотя Группа по EPDP рассмотрела целый ряд примеров использования автоматизации, она смогла согласовать только два для включения в итоговый отчет.[79] Некоторые группы заинтересованных сторон, в том числе GAC, ожидали, что SSAD обеспечит более высокую степень автоматизации и централизации, потому что, как

75 Рек. 6.2.

76 Рек. 6.2

77 *См. сноску 14 выше*

78 Рек. 9.3.

79 *См.* Рек. 9.41 и 9.42 (9.43 и 9.44 относятся к узким категориям запросов только для поля «город» или записей, не содержащих персональные данные).

признали представители органа по защите данных Бельгии, централизованная модель «представляется более качественным и здравым решением с точки зрения обеспечения защищенности субъектов данных».[80] Тем не менее, GAC и некоторые другие группы заинтересованных сторон согласились на использование этой «гибридной», а не централизованной модели, при условии, что окончательные рекомендации включали бы механизм, который обеспечивает гибкость SSAD для развития и изменения без необходимости участия в новых PDP для каждой корректировки, согласующейся с итоговым отчетом.

Рекомендация 18 создает Постоянный комитет из представителей всех групп заинтересованных сторон, участвовавших в EPDP, для принятия этих решений. Тем не менее, GAC считает, что рекомендация 18, которая предусматривает анализ выполнения рекомендаций по политике, похоже, не отвечает цели создания эффективного механизма развития SSAD. В частности, не совсем понятно, подразумевают ли новые примеры использования автоматизации новую политику или реализацию существующей политики. GAC отмечает следующее: если каждый новый пример использования будет считаться новой политикой, требующей нового PDP, на данном этапе неясно, будет ли SSAD эффективно развиваться и, в частности, двигаться в сторону большей централизации. В этом сценарии SSAD может остаться фрагментированной со всеми проблемами, которые сопутствуют такой фрагментации. Поэтому GAC просит GNSO обеспечить, чтобы рекомендации EPDP давали достаточную определенность в этом отношении, позволяя автоматизировать дополнительные элементы, когда выполняется критерий «технически и коммерчески осуществимый и юридически допустимый».

Другими требованиями предусмотрено, что даже для предложений о внесении изменений необходим не только консенсус Постоянного комитета, но и одобрение сторон, связанных договорными обязательствами. Затем рекомендации потребуют утверждения Советом GNSO (в котором отсутствуют представители консультативных комитетов), прежде чем они будут приняты. Такой процесс «развития» может стать сложным и длительным и не подходит для решения вопросов реализации, требующих быстрых и решительных действий.

Финансовая устойчивость

Эти рекомендации могут привести к созданию системы, которая окажется слишком дорогой для своих целевых пользователей, в том числе для тех пользователей SSAD, которые исследуют угрозы кибербезопасности и борются с ними. В рекомендациях говорится, что «субъекты данных НЕ ДОЛЖНЫ нести расходы по раскрытию данных третьим сторонам; расходы на поддержание этой

[80] https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority

системы в первую очередь должны нести податели запросов в SSAD».[81] Хотя GAC признает привлекательность отказа от взимания платы с владельцев доменов, когда другие хотят получить доступ к их данным, GAC также отмечает, что владельцы доменов берут на себя расходы по услугам регистрации домена в целом, когда регистрируют доменное имя. Как недавно отметил SSAC:

> Такие расходы должны охватывать раскрытие информации третьим сторонам, имеющим право на получение скрытых данных, для выполнения законных действий по обеспечению безопасности, стабильности и отказоустойчивости (SSR) и потенциально других законных действий (например, защиты прав), которые выходят за рамки деятельности SSAC. Для общей SSR DNS необходима возможность доступа к таким данным, которая позволяет связываться с владельцами скомпрометированных ресурсов, а также выявлять мошеннические и злонамеренные действия, чтобы приостановить оказание регистрационных услуг преступникам.[82]

Кроме того, GAC отмечает, что большая часть расходов на SSAD связана с повсеместным использованием ручной обработки (вместо автоматизированной), то есть подхода с изначально ограниченной масштабируемостью и высокой стоимостью. Финансовая устойчивость SSAD неразрывно связана с объемом использования ручной обработки в этой системе. Максимально возможное сокращение ручной обработки будет способствовать финансовой устойчивости SSAD.[83] В целом, рекомендации, относящиеся к финансированию SSAD, могут оказаться трудными для реализации и скорее вызывают вопросы, чем дают ответы, в частности: 1) в какой степени ICANN может помочь субсидировать систему; 2) в какой степени регистраторы могут перекладывать расходы по SSAD на своих клиентов; 3) какую роль будут играть податели запросов в установлении и утверждении сборов за использование системы и так далее. GAC считает, что целесообразна «формальная оценка воздействия на пользователя, а также на безопасность и стабильность».[84]

---

81 Рек. 14.2.

82 SAC 111.

83 Еще одна тема, которая могла бы поспособствовать сокращению ручной обработки — это изучение того, какие юридически допустимые механизмы могли бы реализовать стороны, связанные договорными обязательствами, чтобы позволить субъектам данных во время регистрации доменного имени свободно давать согласие на раскрытие данных либо возражать против раскрытия своих данных. Это упростит обслуживание баз данных с защищенной и незащищенной информацией, открывая незащищенные базы данных для более дешевой автоматизированной обработки.

84 *См.* SAC 111.

Проблемы, не рассмотренные в итоговом отчете по фазе 2 EPDP

Точность данных

В уставе Группы по EPDP перед ней была поставлена задача определить «концепцию (концепции) раскрытия […] для (i) решения вопросов, относящихся к злоупотреблениям при регистрации доменных имен, включая защиту потребителей, расследование преступлений в киберпространстве, неправильное использование DNS и защиту интеллектуальной собственности [и] (ii) удовлетворения обоснованных потребностей правоохранительных органов. . . » Эффективность использования регистрационных данных доменного имени для этих целей (на самом деле для любых целей, включая способность сторон, связанных договорными обязательствами, связаться со своими клиентами) зависит от точности данных. Более того, точность регистрационных данных является важным требованием GDPR, и в итоговом отчете по фазе 1 EPDP указано: «*ожидается, что тема точности в отношении соблюдения GDPR будет рассмотрена дополнительно. . .»* Поэтому GAC обеспокоен отсутствием в итоговом отчете каких-либо рекомендаций на эту важную тему.

Как GAC подчеркивал ранее:

> Точность регистрационных данных доменного имени имеет фундаментальное значение как для GDPR, так и для обеспечения безопасности и отказоустойчивости DNS. GDPR, а также другие режимы защиты данных и Соглашение об аккредитации регистраторов ICANN требуют точности данных, и такая точность имеет решающее значение для мандата ICANN по обеспечению безопасности, стабильности, надежности и отказоустойчивости DNS. Как указано в письме ICANN Европейской комиссии от 7 февраля 2018 года: «*[к]ак предусмотрено правовой концепцией защиты данных ЕС и в соответствии с обязанностями сторон, связанных договорными обязательствами с ICANN, персональные данные должны быть точными и актуальными. Необходимо принимать все разумные меры для того, чтобы обеспечить немедленное удаление или исправление неточных персональных данных, с учетом целей, для которых они обрабатываются […]. Для соблюдения принципа качества данных необходимо принимать разумные меры, направленные на обеспечение достоверности любых полученных персональных данных»*.[85]

[85] Комментарий GAC к дополнению отчета по фазе 2.

В соответствии с GDPR важно, чтобы точность и качество данных обеспечивались в зависимости от «цели, для которой они [данные] обрабатываются».[86] Раскрытие неточных данных лишит SSAD смысла и приведет к риску нарушения правил защиты данных. Точность — это основной принцип защиты данных в большинстве законов о защите данных по всему миру. В частности, требование точности предусмотрено статьей 5 GDPR.

Эффективность текущих контрактных требований, направленных на повышение точности WHOIS, представляется неопределенной. Вопросы об эффективности процедур проверки поднимаются в недавних отчетах групп по анализу, таких как одобренные GAC отчеты группы по анализу RDS и группы по анализу CCT.[87] Более того, с 2014 года жалобы на точность данных WHOIS представляют собой самую большую категорию среди жалоб в отношении регистраторов, направленных в отдел по контролю исполнения договорных обязательств ICANN.[88]

Поэтому GAC призывает Совет GNSO поручить действующей Группе по EPDP решить эту проблему, чтобы точность данных была включена в качестве неотъемлемого компонента SSAD.

Физические/юридические лица

В Коммюнике по результатам заседаний GAC на ICANN68 от 27 июня 2020 года, GAC просит Правление как можно скорее получить от GNSO обновленную информацию о ходе работы, направленной на подготовку конкретного плана по продолжению процесса формирования политики для урегулирования нерешенного вопроса, связанного с разграничением физических и юридических лиц. Этот вопрос важен, поскольку правила защиты персональных данных, в том числе GDPR, применяются только к обработке персональных данных физических лиц и защищают их.[89] Информация о юридических лицах не считается

---

86 *См.* GDPR ст. 5(1)(d). *См. также* Руководство Информационной комиссии Великобритании по GDPR, правила для организаций, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/

87 *См., например*, итоговый отчет по результатам 2-й проверки службы каталогов регистрационных данных WHOIS на стр. 49–61 (где отмечается, что уровень недостоверности записей в WHOIS продолжает оставаться высоким и, вероятно, занижается); комментарий Правительственного консультативного комитета к итоговому отчету группы по анализу RDS-WHOIS2 от 23 декабря 2019 г., стр. 5–7; итоговый отчет группы по анализу конкуренции, потребительского доверия и потребительского выбора на стр. 103–06. *См. также* отчет группы по анализу WHOIS (11 мая 2012 года) на стр. 11–13 («низкий уровень точности данных WHOIS является неприемлемым и снижает доверие потребителей к WHOIS — отрасли, где ICANN определяет правила и осуществляет координацию, — и, как следствие, к самой корпорации ICANN»).

88 *См.* годовые отчеты отдела по контролю исполнения договорных обязательств ICANN, подробные сведения о регистраторах, 2014–2019 годы, https://features.icann.org/compliance/dashboard/report-list.

89 Действие GDPR не распространяется на обработку персональных данных юридических лиц и, в частности, предприятий, созданных как юридические лица, включая наименование и форму юридического лица, а также контактные данные юридического лица (декларативная статья (14) GDPR). «Хотя контактные данные юридического лица выходят за рамки GDPR, контактные данные, касающиеся физических лиц, входят в сферу действия GDPR, как и любая другая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу» (*См.* Письмо EDPB в ICANN от 5 июля 2018 года).

персональными данными в соответствии с положениями о защите персональных данных, включая GDPR, если она не позволяет идентифицировать физических лиц. По этой причине стороны, связанные договорными обязательствами, могут сделать такие данные общедоступными, не вызывая опасений по поводу защиты данных. Тем не менее, как отражено в итоговом отчете, регистраторам и операторам регистратур *разрешено*, но не *вменяется в обязанность* проводить различие между регистрационными данными юридических и физических лиц.[90] Эта практика не «обеспечивает в максимально возможной степени постоянную доступность WHOIS»,[91] и отсутствие в итоговом отчете рекомендованных процедур, применимых к этому различию, не соответствует четкой директиве фазы 1 Группы по EPDP и уставу Группы по EPDP.[92]

Влияние маскировки данных, которые по закону разрешено оставлять доступными для общественности, является значительным из-за большого количества доменов, зарегистрированных на юридических лиц. Исследование, проведенное по заказу ICANN в 2013 году, показало, что **юридические лица составили самую большую в процентном отношении категорию владельцев доменных имен**.[93] Один из способов, позволяющих общественности оценить легитимность сайта, а правоохранительным органам выяснить, какие лица за ним стоят, — это обратиться к общедоступной информации о регистрации доменного имени, которая должна включать данные юридических лиц.

Примечательно, что Группа по EPDP получила правовые рекомендации, предлагающие выполнить ряд шагов по снижению риска ответственности.[94] Смысл этих рекомендаций заключается в том, что можно принять широкий спектр

---

90 *См.* раздел 2.3 итогового отчета по фазе 2 EPDP, темы с приоритетом 1 и 2.

91 *См. веб-страницу «Вопросы защиты персональных данных» на сайте ICANN*: https://www.icann.org/dataprotectionprivacy

92 *См. устав Группы по EPDP*: https://gnso.icann.org/sites/default/files/file/field-file-attach/temp-spec-gtld-rd-epdp-19jul18-en.pdf (включая указания группе рассмотреть вопрос о том, следует ли разрешить или вменить в обязанность сторонам, связанным договорными обязательствами, использовать дифференцированный подход к юридическим и физическим лицам, и какой механизм необходим для надежного определения статуса).

93 *См. Исследование вопросов идентификации владельцев доменов в WHOIS*: https://gnso.icann.org/sites/default/files/filefield_39861/registrant-identification-summary-23may13-en.pdf (На основе нашего анализа записей WHOIS, полученных из случайной выборки в размере 1600 доменов из пяти ведущих gTLD,

- 39 процентов (± 2,4 процента) зарегистрированы юридическими лицами
- 33 процента (± 2,3 процента) зарегистрированы физическими лицами
- 20 процентов (± 2,0 процента) были зарегистрированы с использованием услуг сохранения конфиденциальности или регистрации через доверенных лиц.
- Нам не удалось классифицировать оставшиеся 8 процентов (± 1,4 процента), используя данные, доступные в WHOIS.

94 *См.* Рекомендация по вопросам ответственности в связи с самоидентификацией владельца домена как физического или нефизического лица в соответствии с Общим регламентом по защите данных (регламент (ЕС) 2016/679) («GDPR») от компании Bird & Bird (рекомендованные методы включали разработку четко сформулированных уведомлений, чтобы владельцы доменов избегали ошибок; обеспечение понимания владельцами доменов последствий регистрации в качестве юридического лица; и проверку того, что контактная информация не содержит персональных данных).

мер для того, чтобы владельцы доменов правильно указывали свой статус юридического лица. Следует отметить, что некоторые ccTLD (включая ccTLD, расположенные в ЕС) уже делают определенные данные о юридических лицах-владельцах доменов общедоступными, демонстрируя, что такое различие является как юридически допустимым, так и возможным.[95]

Различие в обращении с данными юридических и физических лиц также тесно связано с вопросом автоматизированной обработки. Как отмечалось выше, юридические лица не защищены GDPR. Таким образом, разграничение юридических и физических лиц в процессе регистрации может включать отнесение юридических лиц к категории лиц, данные которых должны обрабатываться автоматически.[96]

GAC считает, что решение проблемы разграничения юридических и физических лиц имеет первостепенную важность для того, чтобы вся модель SSAD соответствовала своей цели и, в то же время, применимым законам о защите данных. Поэтому GAC просит Совет GNSO приложить все возможные усилия для решения этой проблемы. В этой связи GAC повторяет свою просьбу о том, чтобы Группа по EPDP сосредоточила внимание на правовых рекомендациях, предоставленных для разработки разумной политики, позволяющей сохранить общедоступность информации о юридических лицах.

Анонимизированный адрес электронной почты

Использование анонимизированных адресов электронной почты может стать решением в плане защиты идентификационных данных владельца домена и в то же время использоваться лицами, запрашивающими доступ к регистрационным данным доменного имени с легитимными целями. В итоговом отчете среди пунктов, относящихся приоритету 2, указана «возможность использования единого анонимизированного адреса электронной почты для уникальных контактов».[97] Группа по EPDP получила правовые рекомендации, согласно которым анонимизация и псевдонимизация являются полезным методом усиления защиты персональных данных на основе принципа «privacy by design».[98]

---

95 *Например:* Бельгия (.BE), Европейский Союз (.EU), Эстония (.EE), Финляндия (.FI), Франция (.FR), Норвегия (.NO) и другие.

96 В качестве меры предосторожности лица с повышенной правовой защитой могут быть отнесены к группам, для которых не предусмотрена автоматизированная обработка запросов. Сюда могут входить юридические лица, защищенные национальным законодательством (например, законами о банковской тайне), физические лица с особыми юридическими средствами защиты, такими как судебные охранные приказы, статус уязвимого субъекта данных (например, дети, лица, ищущие убежища, другие защищенные классы), а также все национальные общины в юрисдикциях, по умолчанию предоставляющих право на неприкосновенность частной жизни.

97 Итоговый отчет по фазе 2 EPDP на стр. 3.

98 Bird & Bird, правовая рекомендация, «Пакет № 2 вопросов по GDPR, касающихся системы обеспечения стандартизованного доступа к закрытым регистрационным данным и их раскрытия (SSAD), сохранение

GAC хотел бы отметить, что, согласно той же правовой рекомендации, анонимная информация выходит за рамки GDPR.[99] Хотя GAC признает возможность создания связи между анонимной информацией и персональными данными, он согласен с этой правовой рекомендацией в том, что анонимизация — полезный метод повышения конфиденциальности и, соответственно, требует дальнейшего изучения.

В свете вышеизложенного GAC считает, что необходим дополнительный анализ осуществимости, чтобы лучше понять преимущества и риски этого варианта, вместо того, чтобы отклонять его без дальнейшего изучения.

Обязанности контролеров

Возможность использования контролеров, совместно отвечающих за обработку данных, сторонами, связанными договорными обязательствами, и корпорацией ICANN, упоминается в итоговом отчете. Тем не менее, GAC ожидает повышения ясности в плане статуса и роли каждого контролера и стороны, ответственной за обработку данных, в модели SSAD. В частности, наличие конкретных соглашений об обработке данных более четко продемонстрирует, как будет распределяться ответственность между сторонами, связанными договорными обязательствами, и корпорацией ICANN за различные операции по обработке данных. GAC хотел бы обратиться к Совету GNSO с предложением поручить Группе по EPDP продолжить рассмотрение этого вопроса.

Заключение

GAC приветствует добросовестные усилия заинтересованных сторон, персонала и председателей EPDP, участвующих в фазе 2 EPDP, за их постоянную целеустремленность в решении этих важных вопросов общественной политики. У итогового отчета много аспектов, достойных одобрения. Однако GAC считает, что некоторые ключевые рекомендации и нерассмотренные темы требуют дальнейшей работы. Следовательно, Совет GNSO должен поручить Группе по EPDP завершить работу над ними в соответствии с пунктами, поднятыми в этом Заявлении меньшинства. GAC надеется на продолжение взаимодействия с нашими коллегами по этим важным вопросам.

конфиденциальности/регистрация через доверенных лиц и псевдонимизированные адреса электронной почты», (4 февраля 2020 года).

[99] *См.* декларативную статью 26 GDPR.

Заявление об особом мнении Группы некоммерческих заинтересованных сторон (NCSG)

NCSG не согласилась с рекомендациями 22, 20 и 7 по причинам, изложенным ниже.

Рекомендация № 22: Цель № 2

Цель № 2 в рекомендации № 22 в настоящее время сформулирована следующим образом: *«Способствовать сохранению безопасности, стабильности и отказоустойчивости системы доменных имен в соответствии с миссией ICANN».*

NCSG категорически против данной цели. Она слишком расплывчатая и универсальная, что позволяет ICANN обрабатывать регистрационные данные gTLD любым способом, который она сочтет нужным. Для этого корпорации ICANN потребуется всего лишь измыслить причину, соответствующую ее толкованию Устава, как признала Бекки Берр в электронном письме, отправленном Группе по EPDP от имени Правления ICANN.

В этом письме Берр говорит: *«SSR согласно определению в Уставе *является* миссией ICANN. В разделе 1.1 статьи 1 Устава ICANN четко указано, что миссия ICANN заключается в обеспечении стабильной и безопасной работы (SSR) систем уникальных идентификаторов интернета. Сам Устав содержит важные детали относительно объема этой миссии в контексте имен, системы корневых серверов, номеров и протоколов».*

На фазе 1 мы разработали рабочие листы для каждой цели ICANN, подробно описав законные основания и процессы обработки для всех целей. В рамках фазы 2 с этим не удалось справиться. Соответственно, в этой переформулированной Цели № 2 не указывается, почему и кому необходимо раскрывать данные, а также не указывается, почему и как долго их необходимо хранить. Цель № 2, как она сформулирована сейчас в итоговом отчете по фазе 2, также противоречит Принципу ограничения целей GDPR — статья 5(1)(b), который требует, чтобы данные *«собирались для определенных, явных и легитимных целей и не обрабатывались в дальнейшем способом, несовместимым с этими целями»*. Обеспечение стабильной и безопасной работы (SSR) систем уникальных идентификаторов интернета вряд ли можно назвать конкретной или явной целью, и еще менее таковой ее делает толкование Правлением ICANN SSR в контексте компетенции ICANN.

Группа NCSG неоднократно просила Группу по EPDP прийти к общему пониманию того, что входит в миссию ICANN в отношении SSR, и как это соотносится с обработкой ICANN регистрационных данных gTLD. Эти просьбы постоянно

отклонялись, хотя ICANN должна выполнять свою правовую обязанность контролера данных для этой цели.

Группа по EPDP не пришла к пониманию того, каким образом SSR в рамках миссии ICANN применима для этой цели, а ICANN не сообщила, что обладает какой-либо информацией по этому вопросу. Однако, как и в случае с другими законными основаниями GDPR, 6(1)(f) создает дополнительные обязательства со стороны Контроллера перед Субъектом данных, включая защиту его прав и интересов.

В своих рекомендациях по использованию статьи 6(1)(f) в качестве законного основания Управление комиссара по информации Великобритании заявляет, что использовать это законное основание целесообразнее всего тогда, когда (среди прочих обстоятельств) данные людей используются так, как они разумно ожидали, и когда это оказывает минимальное влияние на конфиденциальность. Практически невозможно, чтобы у владельцев доменов gTLD были какие-либо ожидания относительно того, почему и как ICANN будет раскрывать или хранить их данные в соответствии с Целью № 2. Эти неизвестные обстоятельства не были идентифицированы ICANN или Группой по EPDP, и единственный способом, позволяющим владельцу домена понять это в той или иной форме, было бы дополнительное требование к владельцу домена при регистрации доменного имени gTLD стать экспертом в сфере толкования и применения Устава ICANN. Такое ожидание нереально; это выходит за рамки возможностей собственного персонала ICANN, членов Правления и членов Группы по EPDP.

NCSG считает, что эта цель на самом деле не нужна ICANN для выполнения своей миссии; она была помещена туда, чтобы корпорация ICANN могла удовлетворить желания третьих сторон, несмотря на то, что ссылка на законные интересы третьих сторон удалена из пересмотренной рекомендации. Правление ICANN, по-видимому, считает, что это законное основание обеспечивает ей защиту от ответственности, хотя, скорее всего, это не так, при этом полностью игнорируя интересы субъектов данных, которые регламент GDPR призван защищать.

Чтобы эта цель была справедливой по отношению к владельцам доменов, ее необходимо разделить на несколько четко сформулированных целей, идентифицирующих конкретные действия по обработке, которые будут известны и объяснены владельцам доменов в понятной для них форме.

Рекомендация № 20: Поле «город»

Группа NCSG не считает, что были представлены убедительные доводы в пользу изменения рекомендации фазы 1 EPDP в отношении поля «город» с «ДОЛЖЕН скрывать» на «МОЖЕТ скрывать». Предыдущая рекомендация с требованием вымарывать это поле была основана на консультациях с юристами из Bird and Bird, которые высказали следующее мнение:

«3.16 Принимая во внимание все вышеизложенное, соответствующие стороны, вероятно, смогут пройти проверку на соблюдение законных интересов в отношении публикации поля «город». Однако, если исходить из имеющейся на данный момент информации, нам это не представляется очевидным. В частности:

а) потребуется дополнительная информация, чтобы продемонстрировать, что выгоды для правообладателей достаточно значимы, чтобы оправдать всеобщую публикацию данных поля «город» вместо их использования в очень ограниченных случаях; а также

б) необходима дополнительная информация о потенциальном влиянии на права и интересы субъектов данных.

3.17 Соответствующим сторонам затем потребуется тщательно оценить факты и обстоятельства, чтобы определить, перевешиваются ли интересы субъектов данных преследуемыми интересами».

Это ясно указывает на необходимость проверки сбалансированности интересов, чтобы сопоставить законные интересы третьей стороны, стремящейся раскрыть регистрационные данные gTLD, с правами соответствующего владельца домена. Группа NCSG твердо убеждена в том, что ее необходимо проводить в рамках обработки запроса о раскрытии данных через SSAD и не следует объединять с целями ICANN по обработке регистрационных данных gTLD. Именно это было охвачено рекомендациями фазы 1 EPDP.

Этот вывод специалистов компании Bird and Bird был подтвержден в их письме Курту Притцу, где было сказано: *«Результаты правового анализа однозначно указывают на то, что это персональные данные; в принципе их опубликование может быть оправданным с учетом законных интересов правообладателей, если они имеют больший вес, чем интересы физических лиц.*

Результаты рассмотрения конкретных фактов — определение наличия существенных интересов у правообладателей и обеспечение их сбалансированности с интересами владельцев зарегистрированных имен — не являются очевидными».

Все это наводит на мысль о том, что с полем «город» в регистрационных данных gTLD следует обращаться, как со всей другой личной информацией, и ее НЕОБХОДИМО скрывать.

Рекомендация № 7: Цели подателя запроса

Группа NCSG по-прежнему не согласна с включением сноски, в которой указывается, что Директива ЕС по NIS является законодательным примером введения обязательств для соответствующих регулируемых организаций. Этот пример был добавлен к рекомендации на этапе работы Группы по EPDP, на котором итоговый отчет и рекомендации корректировались для достижения максимально возможной поддержки, и, по мнению NCSG, ему не было уделено достаточно времени или внимания для включения в итоговый отчет, а также не были должным образом рассмотрены последствия политики, разрешающей раскрытие данных третьим сторонам.

Кроме того, NCSG не считает, что исключение этого примера окажет какое-либо значимое влияние на способность соответствующих организаций, регулируемых Директивой по NIS или другим аналогичным законодательством, запрашивать закрытые или скрытые регистрационные данные gTLD из SSAD.

Заявление об особом мнении Группы заинтересованных сторон-регистраторов (RrSG)

Итоговый отчет по фазе 2 EPDP представляет собой кульминацию многолетней совместной работы сообщества ICANN. RrSG по-прежнему считает, что в наших общих интересах создать политику и систему, которые уравновешивают требования регистратора по защите данных с потребностями тех, кто полагается на доступ к закрытым регистрационным данным в законных целях.

Регистраторы выражали серьезную озабоченность на протяжении всего процесса фазы 2 EPDP по поводу законности, технической осуществимости и затрат, связанных с разработкой, внедрением и эксплуатацией SSAD. Хотя регистраторы больше поддерживают одни рекомендации, чем другие, все рекомендации в значительной степени взаимозависимы и должны рассматриваться как единое целое, и мы признаем, что конечный результат больше, чем сумма его частей.

Поэтому в духе постоянного компромисса с интересами других заинтересованных сторон мы поддерживаем результаты фазы 2 EPDP и рекомендации настоящего итогового отчета и будем соблюдать принятую в результате согласованную политику.

Мы считаем, что итоговые рекомендации представляют собой достаточное руководство для создания стандартизованной и предсказуемой системы, учитывающей рекомендации фазы 1 EPDP, а также обеспечивают необходимую гибкость в реализации каждым регистратором своих операций с SSAD таким способом, который он считает соответствующим своим юридическим обязательствам и обязательствам, связанным с конфиденциальностью, зачастую в нескольких юрисдикциях.

Мы призываем Совет GNSO и Правление ICANN принять все рекомендации, содержащиеся в отчете, чтобы мы могли перейти к работе по реализации и скорейшему запуску SSAD.

Заявление группы заинтересованных сторон-регистратур об итоговом отчете по фазе II EPDP

Группа заинтересованных сторон-регистратур (RySG) высоко оценивает работу, проделанную на фазе II, признает полезность SSAD для третьих сторон и поддерживает рекомендации, содержащиеся в итоговом отчете. Рекомендации отражают максимальные усилия, которые Группа по EPDP приложила для разработки решения по организации доступа к персональным данным, при котором права субъектов данных на конфиденциальность сбалансированы с законными интересами третьих сторон. Хотя в этом заявлении рассматриваются опасения по поводу определенных аспектов итогового отчета, тем не менее, мы готовы идти на компромиссы, составляющие основу рекомендаций по SSAD. Мы сохраняем оптимизм в отношении будущего развития SSAD.

В течение работы, продолжавшейся больше года, регистратуры твердо придерживались принципов, согласно которым эта система должна (i) отражать сегодняшние реалии законодательства о защите данных, (ii) отдавать приоритет надлежащей защите персональных данных владельца домена перед интересами третьих лиц и (iii) сохранять нашу способность как контролеров выполнять свои юридические обязательства по защите персональных данных. Некоторые выражают недовольство системой, основанной на этих принципах. Тем не менее, мы спокойно отстаиваем эти принципы как лучший способ защиты персональных данных владельцев доменов и выполнения наших обязательств по закону.

RySG участвовала добросовестно

В рамках EPDP была поставлена задача «определить целесообразность преобразования Временной спецификации для регистрационных данных в gTLD в согласованную политику ICANN как есть или с изменениями, при соблюдении требований GDPR и других применимых законов о защите персональных данных».[100] В уставе группы признается, что вспомогательная работа по определению ценности системы для третьих сторон с точки зрения доступа к персональным данным владельца домена начнется только после того, как на основные вопросы «будут даны ответы и они будут окончательно решены в рамках подготовки к составлению первоначального отчета по Временной спецификации».[101] Итоговый отчет по фазе I был выпущен 19 февраля 2019 года, включая подробную и имеющую обязательную силу рекомендацию по стандартизации процесса получения третьими сторонами персональных данных владельца домена.[102]

[100] Окончательный вариант устава EPDP — 19 июля 2018 года, см. здесь.
[101] Окончательный вариант устава EPDP — 19 июля 2018 года, см. здесь.
[102] *См.* итоговый отчет по фазе I EPDP, рекомендация № 18,здесь.

RySG добросовестно участвовала в фазе II для разработки системы на благо третьих сторон, у которых есть законный интерес для доступа к персональным данным владельца домена. Регистратурам не нужна такая система для выполнения своих обязательств по защите персональных данных владельца домена и ответа на запросы третьих лиц, желающих получить эти персональные данные. Сегодня наши участники регулярно и ответственно отвечают на запросы данных без системы SSAD, в соответствии с требованиями отчета по фазе I и нашими обязательствами по закону. Мы продолжим делать это даже после ввода в действие SSAD. К сожалению, SSAD во многом усложняет нашу задачу, создавая необходимость дополнительной обработки и риски для персональных данных владельца домена.

Мы непредвзято выслушали мнения сообществ, которые настаивают на расширении доступа к персональным данным, и участвовали в этом процессе, чтобы найти решения. Хотя мы поддерживаем итоговый отчет и многие компромиссы, на которые пошла группа, по перечисленным ниже причинам у нас есть серьезные опасения, которые потребуют постоянных усилий по мере продвижения сообщества к реализации.

RySG уделяла первостепенное внимание защите данных

Нашей отправной точкой в этих обсуждениях всегда были принципы защиты данных. Защита данных в целом и GDPR в частности «защищают основные права и свободы физических лиц и, в частности, их право на защиту персональных данных».[103] Как недавно подтвердила Комиссия ЕС, «конечной целью GDPR является изменение культуры и поведения всех вовлеченных сторон *на благо людей*».[104] Проще говоря, цель защиты данных — защитить персональные данные людей. Хотя это должно быть бесспорным, наш опыт последних двух лет говорит об обратном.[105]

На практике приоритет защиты данных означает, что субъект данных стоит на первом месте при рассмотрении влияния того, как и кем его данные обрабатываются. Это означает принятие минимизации данных и конфиденциальности по умолчанию в качестве основы, чтобы избежать ненужной обработки персональных данных физического лица. Это означает необходимость отказаться от выполнения требований политики, ограничивающих нашу способность как контролеров выполнять свои юридические обязательства по

[103] GDPR, статья 1 (2).
[104] Европейская комиссия: письмо комиссии Европейскому парламенту и Совету от 24 июня 2020 года, стр. 5 (выделено автором), см. здесь.
[105] В то время как статья 17 Хартии по правам человека признает, что «интеллектуальная собственность должна быть защищена», Европейский парламент пояснил, что осуществление этого права «не должно препятствовать. . . защите персональных данных, в том числе в интернете». См. Директиву 2004/48/ЕС Европейского парламента и Совета от 29 апреля 2004 года о защите прав на интеллектуальную собственность здесь.

адекватному обращению с персональными данными, которые люди доверяют нам.

Помня об этих принципах, мы неоднократно проявляли гибкость и стремились учесть интересы третьих сторон, даже когда это требовало от нас уступок, способных увеличить риск для сторон, связанных договорными обязательствами. Хотя некоторые стороны хотели бы пойти дальше, мы должны провести черту, когда нас просят уступить в тех областях, о которых нам неоднократно говорили, — независимый юрисконсульт фазы II, органы по защите данных и наши собственные члены СРН с опытом в сфере защиты данных в ЕС — что это не разрешено законом или создает значительный риск для субъекта данных.

Целью фазы II была стандартизация процесса запроса персональных данных владельца домена третьими сторонами. Однако неустанное стремление после многих месяцев анализа все же найти способ, обеспечивающий возможность по сути автоматического доступа к персональным данным, не приносит пользы субъектам данных. Мы обеспокоены тем, что попытки добиться автоматического доступа любой ценой в конечном итоге подорвут законность и будущую жизнеспособность SSAD.

Гибридная модель отражает правовую и практическую реальность

Гибридная модель (то есть централизованное получение запросов с децентрализованным принятием решений) — это практическое решение. Мы считаем, что оно устранит многие проблемы их тех, на которые ссылаются податели запросов в связи сохранением того же порядка запроса доступа к персональным данным владельца домена. Самое главное, гибридная модель отражает то, что сегодня реально возможно в рамках закона.

Bird & Bird подтвердила, что ответственность возлагается на контролеров данных, и даже если допустить возможность создания полностью централизованной и автоматизированной системы, в которой стороны, связанные договорными обязательствами, не смогут принимать решения по своему усмотрению «наиболее вероятным результатом и, конечно же, исходной позицией большинства надзорных органов, будет то, что СР являются контролерами».[106] Более того, орган по защите данных Бельгии подчеркнул, что контроль — это фактическая роль, которую сторонам «нельзя просто назначить и, соответственно, просто отказаться от нее. . . на основании совместного соглашения».[107]

Мы принимаем рекомендации Bird & Bird и DPA по этому вопросу, и еще в январе предупредили, что «дальнейшие обсуждения полностью централизованной модели только отвлекают и задерживают нас от своевременного и рентабельного

[106] Фил Брэдли-Шмиг и Рут Бордман (Bird & Bird LLP), «Вопросы 1 и 2: ответственность, механизмы защиты, контролер и сторона, ответственная за обработку данных», 9 сентября 2019 года, стр. 6, 2.18.
[107] Управление по защите данных (Бельгия), письмо Йорану Марби, 4 декабря 2019 года, стр. 3, см. здесь.

выполнения нашей рабочей задачи».[108] К сожалению, даже на поздних стадиях EPDP мы продолжаем слышать предложения о том, как можно централизовать принятие определенных решений в отношении персональных данных владельцев доменов и назначить контролеров в соответствии с нашими рекомендациями по политике.[109]

Ничего не изменилось с тех пор, как Группа по EPDP решила отвергнуть централизацию как не отвечающую предварительному условию уменьшения ответственности сторон, связанных договорными обязательствами.[110]
Мы обеспокоены тем, что некоторые стороны либо не понимают, либо намеренно игнорируют правовые рекомендации, которые не соответствуют предпочтительным для них результатам политики. Ни один из сценариев не идеален для достижения консенсуса по выполнимым рекомендациям политики.

Даже термин «централизация» не совсем точно отражает то, что на самом деле было предложено сторонниками такой модели. Только принятие решений, а не сами данные, всегда были предметом обсуждения «централизованной» системы. Без обладания базовыми данными это не является «централизованной» системой, которая ограничила бы ненужную обработку и повысила бы безопасность субъектов данных. Напротив, такая система добавляет дополнительные ненужные этапы обработки и по умолчанию несовместима с основными принципами минимизации данных и конфиденциальности.

Мы по-прежнему обеспокоены постоянными настойчивыми заявлениями о том, что «централизация» раскрытия персональных данных допустима или реалистична в экосистеме ICANN, несмотря на отсутствие изменений в обстоятельствах, которые изначально привели нас к отказу от централизации. Хотя мы поддержали усилия ICANN по поиску ответов о распределении ответственности в централизованной системе, до сих пор нет указаний на то,

[108] Письмо CPH о последующих шагах от 7 января 2020 года.
[109] См., например, комментарии категории 2 к рекомендации № 9, июль 2020 года, IPC/BC, в которых предлагается «концепция неавтоматизированного централизованного принятия решений в CGM», несмотря на правовые рекомендации и наличие договоренности об использовании гибридной модели: «Согласно полученным правовым рекомендациям, Группа по EPDP рекомендует считать, что для следующих типов запросов юридически допустима в соответствии с GDPR централизованная оценка возможности раскрытия данных Диспетчером центрального шлюза (получение запроса, а также обработка решения о раскрытии), когда такие запросы изначально подлежат обработке и проверке вручную:
· автоматизированные решения о раскрытии данных по запросам в случае очевидного «совпадения домена с товарным знаком»;
· автоматизированные решения о раскрытии данных в случае очевидного фишинга.
При обработке такого решения о раскрытии данных контролером является корпорация ICANN».
[110] «И это означает, по сути, что для создания какой-либо унифицированной модели доступа, вы либо достигаете договоренности с 2500 сторонами, связанными договорными обязательствами, о том, что они считают юридическим риском для себя, либо выступаете с предложениями [так в оригинале], уменьшающими юридическую ответственность сторон, связанных договорными обязательствами». Йоран Марби, стенограмма очного заседания EPDP, 25 сентября 2018 года, стр. 2, см. здесь.

что являющаяся обязательным условием передача ответственности юридически возможна.

Постоянный комитет GNSO

RySG поддерживает концепцию, согласно которой SSAD должна быть гибкой и способной перестраиваться в соответствии с изменившимися юридическими или практическими обстоятельствами. Мы признаем, что SSAD должна быть динамичной и способной адаптироваться к постоянно меняющейся среде административных указаний, судебных решений и новых правил в различных юрисдикциях. Однако мы отвергаем представление о том, что работа Постоянного комитета GNSO должна иметь заранее определенный результат. А именно, мы не можем согласиться с предположением, что SSAD неизбежно будет развиваться в сторону большей централизации и большей автоматизации раскрытия персональных данных в будущем. SSAD должна развиваться на основе фактов и данных, а не предположений и гипотез.

Как было сказано выше, гибридная модель отражает то, что сегодня юридически возможно. Мы не согласились с гибридной моделью, которая когда-нибудь превратится в централизованную модель, потому что мы не можем знать, как будет развиваться законодательство. Мы согласились с гибридной моделью как с решением, позволяющим улучшить существующее положение вещей при одновременной адекватной защите персональных данных людей.

Члены рабочей Группы по EPDP должны определить в своих группах заинтересованных сторон соответствующие ожидания относительно того, как SSAD может измениться с течением времени. Хотя эта система может двигаться в направлении, желательном для некоторых участников EPDP, в равной степени (если не более) вероятно, что система должна будет стать более жесткой, менее автоматизированной или более децентрализованной.[111] Представление развития как движения в одном направлении вместо реагирования на обстоятельства и данные, делает эту систему несостоятельной в глазах некоторых членов сообщества.

Точно так же, хотя мы в целом поддерживаем круг задач Постоянного комитета GNSO, у нас есть серьезные опасения по поводу любых усилий по структурированию этого механизма, направленных на то, чтобы мы уступили контроль над своими юридическими обязательствами в качестве контролеров. Мы сопротивлялись попыткам категорически заявить, что определенные

[111] Многие из наиболее важных недавних решений и руководящих указаний в этой области, по-видимому, предполагают дальнейшие ограничения и усиление контроля за соблюдением, а не ослабление требований. *См., например*, Уполномоченный по защите данных, решение по делу C-311/18 «Максимилиан Шремс против Facebook Ireland Limited («Schrems II»)», аннулирующее систему передачи конфиденциальных данных между ЕС и США; *см. также* письмо Европейской комиссии Европейскому парламенту и Совету от 24 июня 2020 года, в котором содержится призыв к усилению контроля за соблюдением GDPR, а не к ослаблению ограничений здесь).

изменения, такие как добавление новых примеров использования автоматизации, являются реализацией или политикой, потому что нельзя предсказать, какую форму примут будущие руководящие указания по этим вопросам. Если от Европейской комиссии не поступят совершенные, окончательные и безупречные руководящие указания на эту тему, у предложений по автоматизации на основе нового руководства, скорее всего, сохранится остаточный риск, возможность возникновения дополнительных обязательств или необходимости пересмотра соглашений для сторон, связанных договорными обязательствами, или Диспетчера центрального шлюза (CGM).

Мы легко можем представить себе случаи, когда даже простое допустимое руководящее указание по дополнительной автоматизации может потребовать изменения политики. Например, если согласно новому указанию полная автоматизация всегда разрешена при условии, что в каждой организации, которая играет какую-либо роль в обработке данных, есть назначенный сотрудник по защите данных, как это определено в GDPR. В настоящее время наши рекомендации не требуют, чтобы у какой-либо стороны (CGM, орган по аккредитации, регистратуры, регистраторы, податели запросов) был сотрудник по защите данных. В этом сценарии, если дополнительные примеры использования автоматизации были навязаны сторонам, связанным договорными обязательствами, путем реализации, это могло бы значительно увеличить юридические риски сторон, связанных договорными обязательствами, если какая-либо из сторон, участвующих в обработке, не назначит сотрудника по защите данных.

Этот пример показывает, насколько важно не определять заранее, что изменения, которые могут повлечь за собой юридический риск, являются однозначно вопросом реализации, а не политики. Нам, как контролерам, необходима возможность выполнять свои обязательства перед лицами, чьи персональные данные мы обрабатываем.

Полная автоматизация возможна только в очень узких обстоятельствах

RySG поддерживает концепцию автоматизации там, где это «технически и коммерчески осуществимо и допустимо с юридической точки зрения».[112]
Мы рассматриваем эти критерии как необходимые меры предосторожности, направленные на защиту субъектов данных от необоснованной автоматической обработки их данных.

В качестве отправной точки следует признать бесспорным тот факт, что крупномасштабная автоматизация решений, которые влияют на субъектов данных, но от которых они не получают никакой выгоды, как правило, не отвечает насущным интересам субъекта данных. Как гласит GDPR, «субъект данных должен иметь право не подпадать под действие решения, основанного исключительно на

[112] Итоговый отчет по фазе II EPDP, 9.3.

автоматизированной обработке, включая формирование профиля, которое порождает юридические последствия в отношении него или нее или существенно воздействует на него или на нее».[113] Специалисты компании Bird & Bird подтвердили, что из всех возможных примеров использования автоматизации, предложенных группой, только четыре не приводили к юридическим или аналогичным значительным последствиям для субъекта данных.[114]

На основе этой правовой рекомендации мы делаем вывод о том, что только очень узко определенный набор решений не создает юридических или аналогичных значительных последствий для субъектов данных. Точно так же в меморандуме эти примеры использования оцениваются только в рамках GDPR. Таким образом, нам следует с осторожностью делать обобщающие выводы о юридической допустимости, которые заставят стороны, связанные договорными обязательствами, выполнять требования, увеличивающие для них правовой риск.

Мы также обеспокоены тем, что эти четыре примера использования теперь требуют полной автоматизации с самого начала работы SSAD,[115] хотя Группа по EPDP даже не начала участвовать в каких-либо технических дискуссиях о том, как алгоритм может надежно (i) идентифицировать пригодные для автоматизации запросы или (ii) принимать решения надежным, точным и транспарентным образом. На пленарном заседании мы согласились, что автоматизация должна соответствовать трем критериям: (i) техническая осуществимость, (ii) коммерческая осуществимость и (iii) юридическая допустимость.[116] Требуя автоматизации примеров использования в рекомендации 9.4 на основании их юридической допустимости, мы свели эти три важные гарантии к единственной оценке законности таких примеров использования.

Фактически, самое близкое, где мы подошли к какому-либо существенному рассмотрению того, как алгоритм мог бы оценивать и принимать эти решения, — это предположение, что CGM может давать рекомендации по раскрытию данных сторонам, связанным договорными обязательствами, и алгоритм будет обучаться на обратной связи, проверяя, совпадает ли решение о раскрытии данных, принятое стороной, связанной договорными обязательствами, с

[113] GDPR, статья 22.
[114] Итоговый отчет по фазе II EPDP, 9.4: (i) запросы правоохранительных органов в местных или иным образом применимых юрисдикциях, когда 1) имеется подтвержденное законное основание согласно GDPR 6(1)e или 2) обработка должна выполняться в соответствии с исключением, указанным в статье 2 GDPR; (ii) расследование органом по защите данных нарушения законодательства о защите данных, предположительно совершенного ICANN или сторонами, связанными договорными обязательствами, затрагивающего владельца домена; (iii) запрос только данных из поля «город» для оценки необходимости предъявить претензию или для статистических целей; (iv) отсутствие персональных данных в регистрационной записи, которая ранее была раскрыта стороной, связанной договорными обязательствами.
[115] Итоговый отчет по EPDP, 9.4: «Согласно полученным правовым рекомендациям. . . Группа по EPDP рекомендует ОБЯЗАТЕЛЬНО автоматизировать с момента запуска SSAD следующие типы запросов о раскрытии данных, для которых юридическая допустимость полной автоматизации (прием и обработка решения о раскрытии) зафиксирована в GDPR. . .»
[116] Итоговый отчет по фазе II EPDP, 9.3.

автоматизированной рекомендацией.[117] Это не только свидетельствует о неправильном понимании принципов машинного обучения, но у нас есть серьезные сомнения в надежности рекомендаций, подготовленных системой, которая не располагает базовой информацией, составляющей основу наших собственных решений. Даже если наши решения «совпадают» с достаточной регулярностью, эта корреляция не означает, что алгоритм действительно принимает точные и надежные решения.

Чтобы оценить техническую осуществимость этих примеров использования, необходим гораздо более сложный подход к машинному обучению и обучению алгоритмов. Вот почему необходимость технической осуществимости как независимый фактор является важной частью рассмотрения примеров использования автоматизации. Если стороны, которые сейчас должны фактически заниматься оценкой технической осуществимости и построением алгоритма, не могут успешно с этим справиться, нас нельзя принуждать к обязательной автоматизации, поскольку требование о технической осуществимости не выполнено.

Финансовая устойчивость требует внимания

С самого начала фазы II RySG выступала за финансовую оценку предлагаемой SSAD, чтобы предоставить важные данные, которые помогут Группе по EPDP принимать решения. Мы ценим работу, которую проделали сотрудники ICANN, предоставив нам оценку затрат. В свете значительных расчетных затрат ICANN на разработку и поддержку предлагаемой SSAD мы обеспокоены тем, что эта оценка сведена к одной сноске в итоговом отчете, особенно в связи с тем, что мы продолжаем наблюдать сопротивление со стороны других групп на том основании, что пользователи SSAD должны нести расходы по эксплуатации системы.

Повторяя вопрос, который мы неоднократно поднимали во время обсуждения, субъект данных ни при каких обстоятельствах не должен субсидировать возможность получения третьей стороной доступа к его персональным данным**.** SSAD предназначена для обеспечения предсказуемого и стандартизованного доступа к данным и должна финансироваться теми, кто непосредственно пользуется преимуществами такой услуги.

Кроме того, мы поддерживаем проведение ICANN анализа рентабельности для определения финансовой осуществимости такой системы. Учитывая обширную работу на фазе I по созданию стандартизованного процесса, позволяющего третьим сторонам запрашивать данные напрямую у сторон, связанных договорными обязательствами (рекомендация № 18), ни у одной из сторон (субъект данных или сторонний податель запроса) нет предсказуемого процесса для запроса персональных данных. Более того, любой пользователь, не желающий платить за услугу SSAD, по-прежнему сохраняет возможность

[117]Итоговый отчет по фазе II EPDP, 5.1.1, 5.5.

отправлять запросы о раскрытии данных, как установлено на фазе 1, то есть бесплатно для запрашивающей стороны.

На наш взгляд, отсутствие анализа рентабельности также указывает на более серьезную проблему: Группа по EPDP так и не установила — за исключением разрозненных фактов и предположений — какую реальную проблему призвана решить эта система. Мы не видели достоверных данных, свидетельствующих о том, что ответы сторон, связанных договорными обязательствами, на запросы о раскрытии данных являются проблемой. Данные на самом деле свидетельствуют о том, что ответы даются на наиболее правильно сформированные запросы, и что отсутствие ответа обычно связано с (i) неприемлемыми запросами данных, защищенных с помощью услуг сохранения конфиденциальности и регистрации через доверенных лиц, или (ii) отсутствием ответа от подателей запросов, когда требуется дополнительная информация.[118] SSAD не исправит ни одну из этих ошибок подателей запросов.

Проблемы с приоритетом 2 решены

Хотя RySG поддерживает продолжение работы над проблемами с приоритетом 2 (точность, юридические и физические лица и осуществимость уникальных контактов), мы возражаем против утверждения о том, что эти проблемы не были решены на фазе II. Фактически, каждая из этих проблем была подробно рассмотрена, включая подробный анализ компанией Bird & Bird, который позволяет сохранить статус-кво. Мы рекомендуем не начинать дальнейшую работу над этими темами с чистого листа, а вместо этого воспользоваться значительным объемом соответствующей работы, проделанной Группой по EPDP. Мы считаем, что важно обеспечить транспарентность и аккуратность при рассмотрении этих вопросов, чтобы избежать неправильных представлений в сообществе. Например:

Точность — Bird & Bird подтвердила, что точность согласно GDPR является правом для субъекта данных (а не третьих лиц) и обязанностью для контролеров данных.[119] Более того, Bird & Bird подтвердила, что существующие процедуры в Соглашении об аккредитации регистраторов, предназначенные для подтверждения данных владельца домена, недостаточны для выполнения требований к точности, предусмотренных в GDPR.[120]

Юридические и физические лица — мы не оспариваем, что GDPR применяется к данным физических, а не юридических лиц. Мы подчеркнули, что практическая

[118] *См.* Конфиденциальность и законный доступ к персональным данным в Tucows, 13 марта 2020 года, здесь.
[119] Рут Бордман и Катерина Тасси (Bird & Bird LLP), «Рекомендация в отношении принципа точности, который определен в Общем регламенте по защите данных (Регламент (ЕС) 2016/679) («GDPR»): уточняющие вопросы по меморандумам «Юридические и физические лица» и «Точность» от 9 апреля 2020 года.
[120] Рут Бордман и Гейб Малдофф (Bird & Bird LLP), «Рекомендация по значению принципа точности в соответствии с Общим регламентом по защите данных (Регламент (ЕС) 2016/679) («GDPR»)» от 8 февраля 2019 года.

задача состоит в том, чтобы надежно определить, к какой именно категории относятся данные, и как обращаться с записями юридических лиц, которые могут содержать данные физических лиц. Хотя некоторые предлагали опираться на согласие как на механизм снижения риска, Bird & Bird подтвердила, что использование согласия — непростое решение и все же сопряжено со значительным риском ответственности для сторон, связанных договорными обязательствами.[121]

Осуществимость уникальных контактов — мы получили точные правовые рекомендации по этому вопросу, в которых признается, что, хотя псевдонимизация и анонимизация являются полезными мерами по повышению конфиденциальности, публикация маскированных адресов электронной почты не будет соответствовать этим стандартам, поскольку они специально предназначены для обеспечения возможности контакта с людьми.[122] Кроме того, мы отмечаем, что предлагаемая формулировка рекомендаций по этому вопросу была представлена на пленарном заседании 12 марта 2020 года и не встретила возражений, но позже была исключена из итогового отчета.[123]

Контролерам нужна гибкость для выполнения своих обязательств

Мы поддерживаем компромиссы, необходимые для достижения согласия по рекомендации № 8 (Авторизация сторон, связанных договорными обязательствами), но мы обеспокоены тем, что структура стала слишком директивной. То, что начиналось как руководящие принципы того, как раскрывающая организация МОЖЕТ принимать решения, стало жестким в отношении того, как раскрывающая организация ДОЛЖНА принимать решения. Хотя регистратуры поддерживают принцип стандартизации, установленный рабочей группой, в этой политике нет возможности учесть все различия в местных юрисдикциях с различными законами и нормативными актами о конфиденциальности, особенно когда запросы отправляются из-за границы. Следует проявлять осторожность при выполнении и обеспечении соблюдения этой рекомендации, чтобы у раскрывающей данные организация была достаточная свобода действий для учета своих конкретных юридических и

[121] Рут Бордман (Bird & Bird LLP), «Рекомендация по вариантам согласия с целью публикации персональных данных в RDS и требования Общего регламента по защите данных (Регламент (ЕС) 2016/679) («GDPR»)», март 2020 года.
[122] Рут Бордман Bird & Bird, «Пакет № 2 вопросов по GDPR, касающихся системы обеспечения стандартизованного доступа к закрытым регистрационным данным и их раскрытия (SSAD), сохранение конфиденциальности/регистрация через доверенных лиц и псевдонимизированные адреса электронной почты» от 4 февраля 2020 года.
[123]«Группа по EPDP согласилась с проектом текста рекомендации, касающимся как возможности наличия у уникальных контактов единого анонимного адреса электронной почты, так и сокрытия поля «город». Персонал должен включить эти проекты рекомендаций в дополнение по вопросам с приоритетом 2, которое будет опубликовано для общественного обсуждения». Письмо Кейтлин Туберген gnso-epdp-team от 12 марта 2020 года.

юрисдикционных обязательств и она не избегала выполнения этой рекомендации как неосуществимой.

Цель № 2

Новая формулировка Цели № 2 в рекомендации № 22 заменяет первоначальную Цель № 2 из рекомендации № 1 фазы 1 EPDP, которая не была согласована или принята Правлением ICANN. Мы подтверждаем нашу озабоченность, возникшую во время фазы 1[124] в связи с тем, что эта цель не относится к категории законных «целей» согласно определению GDPR.[125] Неясно, позволят ли слова «способствовать поддержанию безопасности, стабильности и отказоустойчивости системы доменных имен в соответствии с миссией ICANN» понять субъекту данных, как его данные будут обрабатываться или почему это необходимо. Принимая во внимание вышеизложенное и поддержку этой цели Правлением,[126] а также дух всего этого намерения, RySG согласилась не возражать против этой цели.

Заключение

Группа RySG обязалась активно и добросовестно участвовать в разработке соответствующих рекомендаций по согласованной политике в отношении доступа к данным владельцев доменов. Мы сосредоточились на том, чтобы такие рекомендации обеспечивали четкий путь к соблюдению GDPR, были коммерчески обоснованными и реализуемыми, учитывали наши различные бизнес-модели и не препятствовали инновациям. В соответствии с этими принципами и принимая во внимание проблемы, подробно описанные выше, мы поддерживаем рекомендации итогового отчета на основе консенсуса. Надеемся на дальнейшее рассмотрение и одобрение Советом GNSO.

[124] Итоговый отчет по фазе I EPDP, Заявление об особом мнении RySG по фазе I, стр. 166, см. здесь.
[125] Руководство ICO по ограничению целей: «Это требование направлено на то, чтобы вы четко и открыто заявляли о причинах получения персональных данных и чтобы то, что вы делаете с данными, соответствовало разумным ожиданиям заинтересованных лиц. Определение ваших целей с самого начала поможет вам нести ответственность за свою обработку и поможет избежать «расширения функций». Это также помогает людям понять, как вы используете их данные, принять решение о том, готовы ли они поделиться своими данными, и отстоять свои права на данные там, где это необходимо. Это очень важно для создания общественного доверия к тому, как вы используете персональные данные». См. здесь.
[126] Письмо Мартина Боттермана Киту Дразеку от 11 марта 2020 года, см. здесь.

SSAC: Заявление об особом мнении относительно итогового отчета по 2-й фазе ускоренного процесса формирования политики в области Временной спецификации для регистрационных данных в gTLD (EPDP) — SSAC 112

Предисловие

Это заявление об особом мнении Консультативного комитета ICANN по безопасности и стабильности (SSAC) относительно итогового отчета по 2-й фазе ускоренного процесса формирования политики в области Временной спецификации для регистрационных данных в gTLD (EPDP).

В центре внимания SSAC находятся вопросы, связанные с безопасностью и целостностью систем распределения имен и адресов интернета. Сюда относятся эксплуатационные (например, связанные с правильной и надежной работой системы опубликования данных корневой зоны), административные (например, связанные с распределением адресов и присвоением номеров в интернете) и регистрационные (например, связанные с услугами регистратур и регистраторов) вопросы. SSAC занимается постоянной оценкой угроз и анализом рисков для служб распределения имен и адресов интернета с целью определения источников основных угроз стабильности и безопасности и дает соответствующие рекомендации сообществу ICANN. SSAC не обладает полномочиями регламентировать, обеспечивать соблюдение или выносить решения. Эти функции исполняют другие органы, и содержащиеся в настоящем документе рекомендации следует рассматривать по существу.

Основные положения

SSAC не может одобрить итоговый отчет по 2-й фазе ускоренного PDP в области Временной спецификации для регистрационных данных в gTLD[127]
(далее «итоговый отчет») в его нынешнем виде.

Во-первых, мы считаем, что в рамках налагаемых Общим регламентом по защите данных (GDPR) ограничений возможна гораздо лучшая система, и EPDP *не* дал результатов, которые способны обеспечить достаточную безопасность и стабильность.

Во-вторых, итоговый отчет не содержит рекомендации в обязательном порядке завершить работу над нерассмотренными вопросами устава группы. SSAC обусловил свое участие и поддержку фазы 2 EPDP выполнением обещания рассмотреть несколько вопросов фазы 1. К сожалению, они не были рассмотрены и остаются без внимания.

[127] См. https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-31jul20-en.pdf.

В-третьих, помимо вопросов, рассмотренных выше, есть некоторые конкретные рекомендации, против которых возражает SSAC, а именно:

- *Рекомендация № 6: Уровни приоритета.* Классификация угроз кибербезопасности как имеющих «Приоритет 3» недостаточна для устранения реальных серьезных онлайн-угроз.
- *Рекомендация № 10: Определение Изменяемых SLA для сроков ответа в SSAD* SSAC обеспокоен длительным временем реагирования, тем, что SLA практически неосуществимы, и что рекомендации по реализации с течением времени могут позволить сторонам, связанным договорными обязательствами, отвечать на запросы данных медленнее.
- *Рекомендация № 12: Требование к раскрытию данных.* SSAC обеспокоен тем, что стороны, связанные договорными обязательствами, могут по своему усмотрению раскрывать личность подателей запросов, вместо того, чтобы делать это только тогда, когда того требует закон о защите данных. Раскрытие личности подателей запросов может поставить их под угрозу и поставить под угрозу расследования.
- *Рекомендация № 14: Финансовая устойчивость.* Рекомендация содержит ошибочные формулировки, которые несправедливо перекладывают расходы на потерпевших, что несовместимо с обычной деловой практикой и противоречит предыдущим рекомендациям SSAC Правлению ICANN. Рекомендация не была составлена в соответствии с процедурами GNSO, не подтверждена доказательствами и может не соответствовать GDPR.

Система стандартизованного доступа к закрытым регистрационным данным и их раскрытия (SSAD), предусмотренная на фазе 2, может улучшить существующее положение вещей, если некоторые рекомендации будут изменены, и если GNSO обязуется завершить работу, которая была отражена в уставе EPDP, но остается без внимания. Как только GNSO гарантирует, что вопросы, относящиеся к разграничению данных физических и юридических лиц, услугам сохранения конфиденциальности/регистрации через доверенных лиц и точности данных, будут незамедлительно изучены в рамках официальной разработки политики, SSAC сможет одобрить итоговый отчет.

1 Введение

SSAC принял участие в EPDP в духе профессионализма и доброй воли, посвятив тысячи часов волонтерской работе на обоих фазах и добросовестно сотрудничая с нашими коллегами из сообщества ICANN.

Как указано в документе SAC111:

> SSAC пошел на компромисс по многим вопросам, как и большинство участников, в интересах продвижения вперед и вывода системы в рабочий режим. Во избежание разночтений настоящим поясняется, что отчет по фазе 2 и его рекомендации в настоящее время далеки от того, что, по мнению SSAC, необходимо и можно сделать для решения проблем безопасности и стабильности в рамках компетенции ICANN. SSAC не считает, что первоначальная версия Системы стандартизованного доступа к закрытым регистрационным данным и их раскрытия (SSAD) будет доставлять данные таким образом и с такой скоростью, которые удовлетворяют многие потребности в операционной безопасности. Мы считаем, что в рамках ограничений, налагаемых GDPR, можно создать лучшую систему. Чтобы уже сегодня появилась возможность двигаться вперед, SSAC поддерживает создание прочного фундамента, который можно своевременно улучшить, вместо того, чтобы стремиться к идеальной системе.[128]

SSAC поддерживает это заявление. Мы не можем одобрить общие результаты фазы 2 в их нынешнем виде.

Мы считаем, что в рамках налагаемых GDPR ограничений возможна гораздо лучшая система, и EPDP не дал результатов, которые способны обеспечить достаточную безопасность и стабильность. Более того, итоговый отчет не содержит рекомендации в обязательном порядке завершить работу над нерассмотренными вопросами устава группы. SSAC обусловил свое участие и поддержку фазы 2 выполнением обещания рассмотреть несколько вопросов фазы 1. К сожалению, они не были рассмотрены и остаются без внимания.

Из двадцати двух рекомендаций в итоговом отчете SSAC возражает против четырех, а именно:

- *Рекомендация № 6: Уровни приоритета.* Классификация угроз кибербезопасности как имеющих «Приоритет 3» недостаточна для устранения реальных серьезных онлайн-угроз.
- *Рекомендация № 10: Определение Изменяемых SLA для сроков ответа в SSAD* SSAC обеспокоен длительным временем реагирования, тем, что SLA практически неосуществимы, и что рекомендации по реализации с течением времени могут позволить сторонам, связанным договорными обязательствами, отвечать на запросы данных медленнее.

[128] См. SAC111, стр. 5, по адресу: https://www.icann.org/en/system/files/files/sac-111-en.pdf.

- *Рекомендация № 12: Требование к раскрытию данных.* SSAC обеспокоен тем, что стороны, связанные договорными обязательствами, могут по своему усмотрению раскрывать личность подателей запросов, вместо того, чтобы делать это только тогда, когда того требует закон о защите данных. Раскрытие личности подателей запросов может поставить их под угрозу и поставить под угрозу расследования.
- *Рекомендация № 14: Финансовая устойчивость.* Рекомендация содержит ошибочные формулировки, которые несправедливо перекладывают расходы на потерпевших, что несовместимо с обычной деловой практикой и противоречит предыдущим рекомендациям SSAC Правлению ICANN. Рекомендация не была составлена в соответствии с процедурами GNSO, не подтверждена доказательствами и может не соответствовать GDPR.

Мы не возражаем против остальных рекомендаций в итоговом отчете. Это не значит, что мы в восторге от всех. Например, SSAC поддерживает идею аккредитации SSAD, поскольку аккредитация — это механизм защиты, разработанный для удовлетворения требований GDPR, обеспечивающий достоверность и документирование законных запросов. Однако мы не знаем, будет ли аккредитация эффективным инструментом. В соответствии с предлагаемой политикой, раскрытие данных будет полностью зависеть от решения каждого регистратора и оператора регистратуры, которые будут сильно различаться по своим методам и стандартам оценки и будут давать неодинаковые, субъективные и непредсказуемые результаты. Предлагаемая политика может не обеспечить эффективную правовую защиту лиц, запрашивающих данные, чьи явно законные запросы отклонены. Таким образом, независимо от строгости введенной программы аккредитации, она может не принести результатов и может не оправдать добросовестные усилия лиц, запрашивающих данные. Это ненадежный результат, и он дает меньше, чем позволяет GDPR.[129]

По нескольким рекомендациям в итоговом отчете не был достигнут консенсус из-за официального возражения со стороны значительного числа участников. Однако некоторые члены сообщества заявляют, что Совет GNSO теперь должен провести одно голосование «за» или «против» всего итогового отчета, одобрив или не одобрив все рекомендации разом. Мы считаем, что такой подход «все или ничего» противоречит процессу достижения консенсуса. Это также нарушит процедуру GNSO, в которой сказано: «Если итоговый отчет содержит рекомендации, относительно которых Группа по PDP не достигла консенсуса,

[129] В июле 2018 года Европейский совет по защите данных отправил корпорации ICANN письмо, в котором подтвердил, что «персональные данные, обрабатываемые в контексте WHOIS, могут быть доступны третьим сторонам, имеющим законный интерес в доступе к данным, при условии соблюдения соответствующих мер безопасности для обеспечения того, чтобы раскрытие информации было соразмерным и ограничивалось необходимым, а также при условии соблюдения других требований GDPR...», письмо Йорану Марби из Европейского совета по защите данных, https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

Совет GNSO должен обсудить целесообразность их утверждения или отправки обратно для дополнительного анализа и работы».[130]

Мы отмечаем, что, хотя в рекомендациях сделана попытка создать общую программу, между ними нет такой тесной взаимозависимости, которая требует голосования «все или ничего». Несомненно, есть возможность изменить рекомендации. Часть рекомендаций (и, конечно, некоторые из множества дополнительных рекомендаций) можно отклонить, оставив остальные нетронутыми. То, что вся работа рухнет без принятия всех рекомендаций или без их утверждения в текущем виде, — это миф. В процедурах GNSO далее говорится, что «Совет GNSO может принять все или любую часть рекомендаций, содержащихся в итоговом отчете», и может контролировать работу по пересмотру рекомендаций. Возможно, придется усердно потрудиться, но это обязанность Совета GNSO и Правления ICANN, которым также необходимо будет рассмотреть результаты. Здесь под микроскопом находится легитимность ICANN и ее процесса с участием многих заинтересованных сторон.

В остальной части этого заявления подробно описаны ключевые вопросы, вызывающие озабоченность SSAC.

2 Невыполненные пункты устава группы

В документе SAC111 SSAC выразил озабоченность тем, что в уставе EPDP есть пункты, которые не были предметом обсуждения и принятия решений. Он отметил, что «важные вопросы, связанные с такими предметными областями, как разграничение данных физических и юридических лиц, услуга сохранения конфиденциальности/регистрации через доверенных лиц и точность данных, могут остаться без внимания EPDP».[131] Эти темы были отложены на фазе 1. SSAC обусловил свое участие и поддержку фазы 2 выполнением обещания рассмотреть эти вопросы. К сожалению, они не были рассмотрены и остаются без внимания. Можно привести следующие примеры:

- Обязательства по изучению вопроса о разграничении физических и юридических лиц в рамках PDP не упоминаются в итоговом отчете.
- В итоговом отчете говорится: «Вывод — Точность и система учета достоверности данных WHOIS: в соответствии с инструкциями Совета GNSO Группа по EPDP не будет больше рассматривать эту тему; вместо этого ожидается, что Совет GNSO сформирует аналитическую группу для

[130] Руководство по процессу разработки политики GNSO, раздел 13 «Обсуждение в Совете», стр. 8. Эта процедура также применима к EPDP. https://gnso.icann.org/sites/default/files/file/field-file-attach/annex-2-pdp-manual-24oct19-en.pdf

[131] SAC111: Комментарий SSAC к первоначальному отчету по 2-й фазе ускоренного процесса формирования политики в области Временной спецификации для регистрационных данных в gTLD, 4 мая 2020 года, стр. 8. https://www.icann.org/en/system/files/files/sac-111-en.pdf

дальнейшего изучения вопросов, касающихся точности и ARS, чтобы содействовать принятию решения о целесообразных последующих шагах для решения выявленных потенциальных проблем». Аналитическая группа — это не обещание заниматься какой-либо работой. В данном случае необходимо принять решения на уровне PDP.

- Проблемы сохранения конфиденциальности и регистрации через доверенных лиц: Работа над вопросами аккредитации провайдеров услуг регистрации через доверенных лиц (PPSAI) в 2016 году не затрагивала важные проблемы, поставленные GDPR и входящие в круг задач EPDP, а рабочие потоки PPSAI и EPDP остаются изолированными. Требуется дополнительная работа.
    - Необходимо обсудить, как затронутые стороны могут запрашивать контактные данные соответствующего домена у аккредитованных ICANN провайдеров услуг сохранения конфиденциальности/регистрации через доверенных лиц, которые являются контролерами данных. Возможность запросить регистрационные данные — в этом весь смысл EPDP и SSAD. Итоговый отчет означает, что ICANN оставляет все домены, защищенные посредством услуг сохранения конфиденциальности и регистрации через доверенных лиц, за пределами SSAD, за пределами своих SLA и механизмов подотчетности.
    - Это входило в устав EPDP. Раздел устава EPDP, где определена миссия и круг задач группы, гласит: «Группа по EPDP должна рассмотреть возможные вспомогательные рекомендации насчет будущей работы GNSO, которая могла бы потребоваться для переоценки соответствующих принципов согласованной политики, в том числе относящихся к регистрационным данным, для приведения в соответствие с применимым законодательством».[132] Группа по EPDP не рассмотрела данный вопрос.

Проблема разграничения данных физических и юридических лиц остается нерешенной отчасти из-за необъяснимой несвоевременности проведения исследования. В отчете по фазе 1 EPDP ICANN было рекомендовано провести «как можно скорее» исследование, в рамках которого будут рассмотрены целесообразность и затраты на разграничение юридических и физических лиц, успешная практика разграничения юридических и физических лиц в других отраслях и организациях, а также риски конфиденциальности для владельцев зарегистрированных имен при разграничении юридических и физических лиц

[132] Окончательный вариант устава EPDP – 19 июля 2018 года. См. здесь: https://community.icann.org/display/EOTSFGRD/EPDP+Team+Charter?preview=/88574674/90767676/EPDP%20FINAL%20Adopted%20Charter%20-%2019%20July%202018.pdf.

(рекомендация № 17.2).[133] 15 мая 2019 года Правление ICANN приняло эту рекомендацию и поручило персоналу ICANN выполнить проект в качестве вклада в работу фазы 2 EPDP.[134]

Произошло две ошибки:

1. Отчет об исследовании был передан в EPDP 8 июля 2020 года, *после* завершения подготовки итогового отчета, то есть слишком поздно, чтобы уделить должное внимание вопросу разграничения юридических и физических лиц.
2. В отчете об исследовании не рассматриваются некоторые из наиболее актуальных и очевидных примеров, например как и почему данные физических и юридических лиц собираются и публикуются в реестрах недвижимости, реестрах компаний и реестрах товарных знаков на территории ЕС; и как в таких реестрах за пределами ЕС обрабатываются данные субъектов, проживающих в ЕС. Хотя в отчете было указано, что «большинство операторов ccTLD в ЕС продолжают публиковать некоторые (а иногда и все) поля контактных данных для доменов, зарегистрированных юридическими лицами»,[135] отчет не содержал подробностей, таких как список ccTLD и перечень публикуемых данных.

SSAC просит Совет GNSO и Правление ICANN объяснить, почему отчет был представлен так поздно и почему резолюция Правления не была выполнена для предполагаемых бенефициаров — участников EPDP из сообщества. Для обоснованного принятия будущих решений может потребоваться доработка отчета с целью включения в его состав отсутствующего анализа, упомянутого выше, и другой важной информации.

Как отмечено в документе SAC111: «GNSO создает четкие уставы, чтобы рабочие группы и их участники понимали, какие отчеты необходимо представить. У GNSO имеются стандарты и процедуры для рабочих групп, разработанные для предсказуемого и беспристрастного выполнения работ, и группы, входящие в состав рабочих группах, должны быть в состоянии выполнять обязательства, которые они берут друг перед другом... Когда установленные процессы не работают и критически важные элементы не рассматриваются, это ставит под

[133] https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf.
[134] См. резолюцию Правления ICANN от 15 мая 2019 года, https://features.icann.org/consideration-gnso-epdp-recommendations-temporary-specification-gtld-registration-data и сопроводительный оценочный отчет Правления ICANN, рекомендация № 17, стр. 5, https://www.icann.org/en/system/files/files/epdp-scorecard-15may19-en.pdf
[135] Разграничение юридических и физических лиц в службах каталогов регистрационных данных доменных имен. https://mm.icann.org/pipermail/gnso-epdp-team/attachments/20200708/5f72ece1/Rec17.2_Legal-Natural_8jul201-0001.pdf.

угрозу законность разработки политики ICANN по критически важным вопросам, представляющим глобальный интерес».[136]

3 Общие проблемы с установлением приоритетов и реагированием на запросы

Эти две рекомендации тесно связаны: рекомендация № 6 обеспечивает концепцию «приоритета» запросов о раскрытии данных, а рекомендация № 10 очень точно определяет ожидаемый срок ответа соответствующих сторон, связанных договорными обязательствами, на такие запросы. Предоставление рекомендаций по политике, которые создают дифференцированные приоритеты для различных типов запросов о раскрытии данных, полезно, поскольку некоторые данные могут потребоваться почти немедленно для устранения проблем, которые чувствительны к срокам и (или) очень важны по своему характеру, в то время как другие не связаны со срочными или неотложными потребностями. Предоставление сторонам, связанным договорными обязательствами, и другим участникам процесса раскрытия данных, руководящих указаний по ожидаемым срокам ответов (включая статус запросов и запрашиваемые данные, если они утверждены) также очень полезно для создания системы, в которой соблюдаются принципы согласованности и подотчетности.

К сожалению, полученные рекомендации выходят далеко за рамки необходимых рекомендаций по политике и предписывают очень конкретные детали реализации этой политики. Эти детали жесткие, недостаточно хорошо учитывают все нюансы и плохо спроектированы для удовлетворения многих наиболее насущных потребностей в доступе к данным RDS, особенно в сфере кибербезопасности. Несмотря на благие намерения, включение такого подробного плана реализации в политику вполне может в итоге привести к созданию сложной, трудной в обслуживании системы, которая перегружает стороны, связанные договорными обязательствами, по многим категориям запросов, в то время как многие податели других типов запросов будут обслуживаться удручающе плохо.

SSAC поддерживает общие цели по созданию концепции, в которой определены приоритеты и ожидания в отношении ответов. Однако работу по реализации следует оставить группе по реализации. В эту группу должны входить представители сторон, связанных договорными обязательствами, которые будут предоставлять данные в ответ на запросы, сторон, которые обычно чаще всего запрашивают данные, и персонал ICANN, которому будет поручено управление SSAD и надзор. Эта группа может определить приоритеты и сроки реагирования, которые должны отражать обычно наблюдаемые примеры использования и их

[136] SAC111: Комментарий SSAC к первоначальному отчету по 2-й фазе ускоренного процесса формирования политики в области Временной спецификации для регистрационных данных в gTLD, 4 мая 2020 года, стр. 8. https://www.icann.org/en/system/files/files/sac-111-en.pdf

относительную срочность в отношении своевременности, воздействия и (или) других взаимно согласованных факторов. Список в рекомендации № 6.1.1 для запросов с приоритетом 1 в отчете является отправной точкой для таких обсуждений, но ни в коем случае не является полным. Окончательные рекомендации по реализации для поддержки этой концепции должны быть рассмотрены и утверждены советом GNSO. Со временем эти факторы могут быть пересмотрены и скорректированы с использованием механизма развития, предусмотренного в рекомендации № 18 или эквивалентной рекомендации, которая будет принята в итоге.

4 Возражение против рекомендации № 6 об уровнях приоритета

В отсутствие лучшего подхода к вопросу о приоритетах и SLA, как указано выше, SSAC возражает против 6.1 и 6.2.

Классификация угроз кибербезопасности как имеющих «Приоритет 3» недостаточна для устранения реальных серьезных онлайн-угроз. Эта классификация не учитывает некоторые из наиболее серьезных современных онлайн-атак, которые требуют быстрого реагирования. Такие атаки приводят к огромным финансовым последствиям и разглашению миллионов конфиденциальных личных записей в интернете, например программы-вымогатели, сети кражи данных и масштабные DDoS-атаки с целью вымогательства. Эта система классификации нуждается в доработке, чтобы обеспечить своевременность реагирования и учесть последствия различных видов атак. По меньшей мере, такая система создавала бы концепцию политики, которая может направлять практические процессы реализации для удовлетворения потребности в своевременном получении данных в зависимости от множества факторов. Если рекомендация № 6 не будет обновлена с учетом необходимости своевременного реагирования на различные атаки, то необходимы более жесткие ограничения в соответствии с рекомендацией № 10 (Определение Изменяемых SLA для сроков ответа в SSAD) для предоставления данных для поддержки усилий по реагированию на такие атаки. SSAC ранее изложил дополнительное обоснование этого подхода в SAC111, раздел 3.2[137].

5 Возражение против рекомендации № 10 об определении Изменяемых SLA для сроков ответа в SSAD

В отсутствие лучшего подхода к вопросу о приоритетах и SLA, как указано выше, SSAC возражает против рекомендации № 10. Хотя у рекомендации хорошая цель, SSAC не поддерживает эту рекомендацию в ее текущей формулировке. Ее логика ошибочна, и она не обеспечивает разумного SLA для реагирования на угрозы безопасности. Частично это связано с тем, что угрозам безопасности присвоен

[137] https://www.icann.org/en/system/files/files/sac-111-en.pdf

«Приоритет 3» в рекомендации № 6 (Уровни приоритета).[138]. Это слишком медленное реагирование для устранения инцидентов в сфере кибербезопасности.[139]

Цель SLA на фазе 1 — 5 (пять) дней. Но в разделе 10.11 сказано: «На фазе 2 целевые показатели стороны, связанной договорными обязательствами, для запросов SSAD с приоритетом 3 составляют 10 (десять) рабочих дней». К сожалению, на фазе 1 обязательное для соблюдения SLA вообще не рассматривалось, и SLA, для которого предусмотрены штрафные санкции, вступает в силу только на фазе 2. SLA фазы 2 позволяет сторонам, связанным договорными обязательствами, по мере накопления опыта реагировать *медленнее*, чем на фазе 1, а не быстрее. Десять дней — это слишком много для безопасности и стабильности. Это предложение не претерпело значительных изменений со времени предварительного отчета, и в то время SSAC представил свое возражение против этого противоречивого подхода в разделе 3.2 SAC111:

> Эти цели не совпадают с причинами создания SSAD. Запросы в сфере кибербезопасности обычно имеют высокий приоритет. Обычно они носят оперативный характер и предназначены для предотвращения активно и непрерывно наносимого ущерба множеству жертв из числа пользователей во время атак (например, при распространении вредоносного ПО и фишинге). Запросы, направленные на оперативное обеспечение кибербезопасности, не менее срочны, чем запросы URS. Кроме того, общая модель SSAD предполагает, что запросы, направленные на обеспечение кибербезопасности, будут отправляться аккредитованными сторонами в рамках подотчетной системы, что снижает необходимость в расширенной проверке. SSAC рекомендует перевести запросы, связанные с оперативным обеспечением безопасности (от аккредитованных сторон), в категорию с уровнем приоритета 2. Если объем запросов, поступающих в рамках обеспечения кибербезопасности, является предметом беспокойства сторон, связанных договорными обязательствами, то разумным компромиссом будет ответ в течение 3 (трех) рабочих дней.
>
> Податели запросов и стороны, связанные договорными обязательствами, со временем обретут уверенность и повысят эффективность, поэтому нет причин впоследствии увеличивать срок ответа. Таким образом, на фазе 2 нет смысла увеличивать срок, в течение которого контролер данных должен отправить ответ (как определено в SLA) по сравнению с фазой 1 для запросов с любым уровнем приоритета. Эти сроки должны оставаться

[138] За исключением случаев, связанных с «непосредственной угрозой жизни, серьезными телесными повреждениями, критически важной инфраструктурой (онлайн и офлайн) или эксплуатацией детей».
[139] Лишь небольшой процент проблем безопасности и киберпреступлений достигнет высокой планки приоритета 1, который охватывает «непосредственную угрозу жизни, серьезные телесные повреждения, угрозу критически важной инфраструктуре (онлайн и офлайн) или эксплуатацию детей».

такими же или уменьшаться с течением времени для одинакового приоритета.

SSAC обеспокоен тем, что SLA практически невыполнимо и рекомендации по реализации вызывают проблемы. SLA для времени реагирования включает в себя скользящее среднее всех значений времени реагирования. Сторона, связанная договорными обязательствами, может быстро отклонить все запросы данных или может немедленно запросить дополнительную информацию по всем запросам. Это приведет к очень низкому среднему времени ответа стороны, связанной договорными обязательствами. И это позволило бы стороне, связанной договорными обязательствами, затягивать рассмотрение других запросов на длительный срок, прежде чем будет нарушено SLA по реагированию. Такие автоматизированные действия не запрещены рекомендацией № 8.1. Поэтому важно, чтобы отдел по контролю исполнения договорных обязательств ICANN мог определять, рассматривают ли стороны, связанные договорными обязательствами, запросы и реагируют ли они в соответствии с рекомендацией № 8. Нам неизвестно, каким образом персонал корпорации ICANN мог бы определить это, поэтому мы сомневаемся, что соблюдение SLA можно проконтролировать на практике.

6 Возражение против рекомендации № 12 о требовании к раскрытию данных

Рекомендация № 12.2 позволит сторонам, связанным договорными обязательствами, раскрывать личности подателей запросов в любое время, когда они пожелают, даже разрешая «выдачу» подателей запросов в рамках рутинной и автоматизированной процедуры. Таким образом, рекомендация может превосходить или противоречить совету, полученному ICANN от Европейского совета по защите данных (EDPB), в котором говорится, что нет необходимости сообщать личности подателей запросов субъектам данных (владельцам доменов). Раскрытие личности подателей запросов поставит под угрозу расследования и может поставить под угрозу безопасность и права подателей запросов, а также может затруднить использование запросов по статье 6, что, безусловно, не входило в цели GDPR. Стороне, связанной договорными обязательствами, возможно, потребуется проводить проверку сбалансированности интересов, чтобы раскрыть личность подателя запроса, поскольку сторонние податели запросов являются субъектами данных и также имеют права в соответствии с GDPR.

Рекомендация № 12 должна запрещать сторонам, связанным договорными обязательствами, раскрывать личности подателей запросов, пока это не станет *обязательным* в рамках действующего законодательства. Мы рекомендуем, чтобы контролеры данных соблюдали закон и не делали большего. Повторяя SAC055 и SAC101v2, «SSAC считает, что у правоохранительных органов и специалистов по безопасности есть законная потребность в установлении

реальной личности стороны, ответственной (сторон, ответственных) за доменное имя. Такой доступ должен соответствовать требованиям законодательства».

В своем письме от 10 мая 2018 года ICANN спросила Европейский совет по защите данных (EDPB):

> «a) Должна ли личность подателя запроса в WHOIS быть видна владельцу домена или другим третьим лицам?»…
>
> «b) Должен ли владелец домена или третьи лица знать о запросах правоохранительных органов на доступ к закрытым данным WHOIS?»

EDPB ответил:

> «Обеспечение отслеживания доступа с помощью соответствующих механизмов регистрации не обязательно требует активной передачи (принудительной отправки) информации журнала [личностей подателей запросов] владельцу домена или третьим сторонам. ICANN и другие контролеры, участвующие в системе WHOIS, должны гарантировать, что зарегистрированная информация не будет раскрыта неавторизованным лицам, в частности, чтобы не поставить под угрозу законную деятельность правоохранительных органов».[140]

GDPR требует, чтобы контролеры данных, предлагая свои услуги, в принципе информировали субъектов данных о *типах* сторон, которые могут обрабатывать их данные. GDPR не требует активного уведомления субъектов данных о поступлении запросов на раскрытие их данных. GDPR может требовать только, чтобы контролеры данных передавали сведения о личности сторонних подателей запросов субъектам данных, *если и когда субъект данных запрашивает эту информацию*.

Раскрытие личности подателя запроса создает некоторые проблемы для сторон, связанных договорными обязательствами. Раскрытие личности подателей запросов наносит ущерб использованию требований статьи 6 GDPR. Это может серьезно повредить сбору данных, необходимых для легитимных целей в соответствии с GDPR, таких как снижение киберпреступности, защита жертв и расследования, которые могут привести к судебным разбирательствам или мерам принуждения. Очевидно, что в GDPR сделано исключение в отношении права субъекта данных на получение информации, когда разоблачение или уведомление может повлиять на способность стороны (например, стороннего

[140] Письмо Андреа Елинек, председателя EDPB, Йорану Марби, генеральному директору ICANN, 5 июля 2018 года. https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

запрашивающего лица) достичь своих легитимных целей.[141] Это может произойти в контексте расследования.[142]

Эти вопросы не рассматривались Группой по EPDP, и Группа по EPDP не получила по ним надлежащих правовых рекомендаций. Нам интересно, какие права есть у подателей запросов — они являются субъектами данных, и их данные также защищены GDPR. Можно ли принудить подателя запроса, желающего сделать запрос по статье 6(1)f, отказаться от своих прав на конфиденциальность в пользу субъекта данных или контролера данных? (GDPR гласит, что ни один субъект данных не может быть принужден к отказу от своих прав на конфиденциальность в качестве условия контракта.) И было бы несправедливо, если бы сторона, связанная договорными обязательствами, сообщала подателю запроса о том, что она раскрыла личность подателя запроса владельцу домена, тем самым уведомив обе стороны.

SSAC передал свои вопросы по этим проблемам Группе по EPDP и ее юридической подгруппе, предложив переадресовать эти вопросы стороннему юрисконсульту. Группа по EPDP отклонила эту просьбу, и вопросы не были отправлены Bird & Bird. В результате Группа по EPDP не располагает всей необходимой информацией и допускает перегибы, которые не являются необходимыми и нанесут вред.

7 Возражение против рекомендации № 14 о финансовой устойчивости

SSAC отклоняет рекомендации № 14.2 и 14.6.

Следующая формулировка в 14.2 недопустима:

> Цель состоит в том, чтобы SSAD была финансово самодостаточной и не требовала никаких дополнительных сборов с владельцев доменов. Субъекты данных НЕ ДОЛЖНЫ нести расходы по раскрытию данных третьим сторонам; расходы на поддержание этой системы в первую очередь должны нести податели запросов в SSAD. Кроме того, субъекты данных НЕ ДОЛЖНЫ нести расходы по обработке запросов о раскрытии данных, которые были отклонены сторонами, связанными договорными обязательствами, после оценки запросов, отправленных пользователями SSAD. ICANN МОЖЕТ внести свой вклад в (частичное) покрытие расходов на содержание центрального шлюза. Настоящим поясняется: Группа по EPDP понимает, что владельцы доменов в конечном итоге являются источником большей части доходов ICANN. Этот доход сам по себе не нарушает

[141] GDPR, статья 14, параграф 5.

[142] Управление Комиссара по информации, «Право на получение информации: существуют ли исключения?» https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/are-there-any-exceptions/#:~:text=There%20is%20no%20automatic%20exception,a%20specific%20exception%20or%20exemption.

ограничение, что «[с]убъекты данных НЕ ДОЛЖНЫ нести расходы по раскрытию данных третьим сторонам.

1) Податели запросов не должны нести основные расходы по обслуживанию системы.[143] Конечно, податели запросов обязаны оплачивать стоимость аккредитации и сохранения своего доступа к системе. Но текущая формулировка 14.2 обязывает жертв и защитников покрывать расходы на эксплуатацию системы, что несправедливо и потенциально угрожает безопасности в интернете. Как отметил SSAC в документе SAC101v2, «несвободная система [в которой податели запросов должны платить за запросы] может сделать стоимость запросов, необходимых для обнаружения и смягчения злоупотреблений доменом, чрезмерно высокой и будет очень сложна в эксплуатации».

2) Это заявление слишком широкое и может быть неверно истолковано: «Субъекты данных НЕ ДОЛЖНЫ нести расходы по раскрытию данных третьим сторонам». Затем его формулировка была изменена на следующую: «Настоящим поясняется: Группа по EPDP понимает, что владельцы доменов в конечном итоге являются источником большей части доходов ICANN. Этот доход сам по себе не нарушает ограничение, что «[с]убъекты данных НЕ ДОЛЖНЫ нести расходы по раскрытию данных третьим сторонам».

Эта формулировка по-прежнему не позволяет регистраторам перекладывать расходы на программу SSAD на владельцев доменов в ходе обычной деятельности. Стороны, связанные договорными обязательствами, обычно рассматривают затраты на выполнение своих основных обязанности как издержки ведения своего бизнеса и могут переложить эти затраты на своих клиентов.[144] Но пункт 14.2 это запрещает. Ни один предыдущий PDP не защищал владельцев доменов от перекладывания на них затрат, связанных с «основными» регистрационными услугами или реализацией согласованной политики. Ни один из предыдущих PDP не пытался манипулировать действием рыночных сил, как это предлагается в рекомендации № 14.

Если цель состоит в том, чтобы просто запретить регистраторам взимать плату за обслуживание с владельца домена, когда третья сторона фактически запрашивает данные этого владельца домена, просто скажите об этом четко и кратко.

3) SSAD не обязательно должна быть «финансово самодостаточной», и EPDP не дает достаточных оснований для этого. Как было сказано ранее,[145] SSAC считает, что «при введении сборов за доступ к RDDS или существенном изменении таких сборов в будущем необходимо надлежащим образом оценить воздействие на пользователей, безопасность и стабильность. Группа по EPDP не изучила

[143] См. также рекомендацию № 14.6.
[144] См. SAC101v2, раздел 5.4.
[145] См. SAC101v2 и SAC111.

связанные с этим вопросы, как было предложено, и не обосновала рекомендацию по политике в соответствии с требованиями процедуры GNSO. Формулировка пункта 14.2 также игнорирует рекомендации SSAC Правлению ICANN, которые Правление передало GNSO. Все эти факторы делают рекомендацию № 14 преждевременной.

23 июня 2019 года Правление ICANN рассмотрело документ SAC101v2 и передало свои рекомендации Совету GNSO для рассмотрения и включения в состав работ фазы 2 EPDP. В рекомендации говорилось: «При введении сборов за доступ к RDS или существенном изменении таких сборов в будущем необходимо надлежащим образом, используя официальный процесс разработки политики (PDP), оценить воздействие на пользователей, безопасность и стабильность. И: Правление ICANN должно обеспечить официальную оценку рисков безопасности, связанных с политикой в отношении регистрационных данных, в рамках подготовки исходных данных для процесса разработки политики. Также следует выполнить отдельную оценку риска применительно к реализации этой политики».[146]

Эти оценки воздействия на пользователя и на безопасность никогда и нигде не проводились. В рамках EPDP неуместно возлагать затраты на подателей запросов в SSAD без оценки воздействия на них и без оценки воздействия на безопасность DNS.

Когда Группа по EPDP формулировала рекомендацию № 14.2, она не следовала процедурам GNSO, и поэтому рекомендация не может считаться оправданной как предложение по политике. В Руководстве GNSO по PDP прямо говорится: «Группа по PDP должна тщательно рассмотреть последствия для бюджета, возможность реализации и (или) осуществимость своих предлагаемых информационных запросов и (или) последующих рекомендаций». Руководство по PDP GNSO также требует, чтобы в первоначальный отчет было включено «заявление по результатам обсуждения рабочей группой последствий предлагаемых рекомендаций, которое может затрагивать такие сферы, как экономическое влияние, конкуренция, деятельность организации, неприкосновенность частной жизни и другие права, масштабируемость и осуществимость».

Но в рамках EPDP не изучалось влияние на *подателей запросов* с точки зрения бюджета и реализации. Группа по EPDP не занималась изучением общего влияния с точки зрения бюджета и реализации, за исключением получения от персонала корпорации ICANN расплывчатой и недокументированной оценки затрат на запуск центральной системы. В рамках EPDP никогда не изучались аспекты конкуренции и ведения деятельности, а также не оценивалось, как плата

[146] Резолюция Правления от 23 июля 2019 года: https://features.icann.org/consideration-ssac-advisory-regarding-access-domain-name-registration-data-sac101

за доступ повлияет на безопасность и стабильность. Формулировка пункта 14.2 должным образом не изучена и не обоснована.

После общих заявлений о политике в рекомендации № 14.2 в итоговом отчете сказано, что все детали должны быть проработаны на этапе реализации. Этап реализации — неподходящее время для рассмотрения таких фундаментальных вопросов политики, и при любом варианте реализации придется соблюдать ошибочные и неоправданные принципы, которые в настоящее время изложены в пункте 14.2.

4) Нет необходимости заставлять запрашивающих данные лиц «нести основные расходы по обслуживанию системы». Эффективная альтернатива — использование средств ICANN.

SSAD — это многоуровневая система доступа, которую сообщество ICANN давно ожидало как одну из функциональных возможностей системы RDS.[147] Службы регистрационных данных всегда были одной из основных служб, предоставляемых сторонами, связанными договорными обязательствами, в качестве общедоступного ресурса.[148] Ожидаемый в течение нескольких лет многоуровневый/дифференцированный доступ теперь стал необходимым из-за изменений в законодательстве. SSAD будет удовлетворять эту основную потребность, отвечающую общественным интересам. Поэтому вызывает удивление, что рекомендация № 14 по сути запрещает использовать сборы ICANN за регистрацию доменов для поддержки работы системы.

Использование средств ICANN представляется в высшей степени соответствующим миссии ICANN. Временная спецификация также напоминает нам, что «ICANN, как правило, стремится в максимально допустимой степени поддерживать существующую систему WHOIS», и «миссия ICANN подразумевает непосредственное содействие обработке данных третьими лицами с правомерными и надлежащими целями, связанными с правоохранительной деятельностью, конкуренцией, защитой потребителей, доверием, безопасностью, стабильностью, отказоустойчивостью, умышленным злоупотреблением, суверенитетом и защитой прав». Подробнее об обязательствах ICANN и ее миссии см. в документе SAC101v2, раздел 5.4.[149]

[147] Сообщество ICANN рассматривало многоуровневый или дифференцированный доступ как ожидаемую функцию служб каталогов регистрационных данных. Например, протокол RDAP был разработан специально для обеспечения многоуровневого/дифференцированного доступа, поскольку сообщество понимало, что законы о конфиденциальности могут требовать, чтобы определенные виды данных передавались только авторизованным пользователям. Теперь SSAD рассматривается как способ предоставления данных, требующих особенного внимания (и может использовать или не использовать RDAP).
[148] См. SAC101v2, раздел на стр. 4.
[149] https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf

Аналогичным примером является Централизованная служба файлов корневой зоны (CZDS), которую ICANN создала и поддерживает на средства ICANN. ICANN делает это, потому что файлы зон являются критическим ресурсом, используемым в легитимных целях различными пользователями. И CZDS приносит пользу не только своим пользователям, но и сторонам, связанным договорными обязательствами, которые получают удобный способ управления подписками на файлы зон. SSAD создает аналогичную ситуацию и должна будет приносить пользу как запрашивающим данные лицам, так и сторонам, связанным договорными обязательствами.

5) Это предложение было добавлено в рекомендацию № 14 в последнюю минуту: «Кроме того, субъекты данных НЕ ДОЛЖНЫ нести расходы по обработке запросов о раскрытии данных, которые были отклонены сторонами, связанными договорными обязательствами, после оценки запросов, отправленных пользователями SSAD». Непонятно, зачем вообще потребовалось это дополнение, и оно ставит под ставит под сомнение возможность каким-либо образом переложить затраты по оценке запросов данных на владельцев доменов, даже в ходе обычной деятельности.

6) В рекомендации сказано: «Центральному шлюзу ЗАПРЕЩАЕТСЯ взимать отдельную плату с субъектов данных за запрос или раскрытие их данных третьим сторонам». Мы не понимаем, каким образом центральный шлюз мог бы взимать плату с владельцев доменов. У центрального шлюза нет деловых отношений с владельцами доменов.

7) Обычно причиной запроса данных третьими сторонами являются действия *владельцев доменов*.

8) SSAC не знает, нарушит ли рекомендация № 14 положения GDPR.

Рекомендация № 14 (включая пункт 14.6) предусматривает уплату сборов за запросы данных лицами, запрашивающими данные. Плата за использование — единственный способ создать модель «возмещения затрат», предусмотренную в рекомендациях 14.2 и 14.6, или эксплуатировать систему без перекладывания затрат на владельцев доменов/субъектов данных.

Согласно GDPR, если субъекты данных хотят получить, обновить или потребовать удаления своих данных, с них не может взиматься плата за это.[150] Согласно GDPR, третьи стороны с законными интересами могут получать данные, когда их право

[150] См. статьи 15 и 57(4) GDPR и Управление комиссара по информации: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ GDPR позволяет взимать плату с субъектов данных только в том случае, если их запросы являются «явно необоснованными или чрезмерными». В SSAD необоснованные или чрезмерные запросы данных не допускаются и будут отклонены.

на получение данных перевешивает интересы субъекта данных. В SSAD такие запросы обычно отправляются третьими сторонами, поскольку они могут обоснованно заявить, что их права нарушаются субъектом данных (владельцем домена). Группа по EPDP не проверяла, разрешены ли сборы за сторонние запросы данных в соответствии с GDPR и при каких обстоятельствах. Группа по EPDP не обращалась за правовыми рекомендациями по этому вопросу даже после того, как SSAC предложил направить вопрос для получения сторонней юридической помощи.

Этой проблемы можно избежать, если ICANN субсидирует SSAD.

8 Прочие комментарии

Ниже приведены комментарии к другим рекомендациям, против которых SSAC не возражал, но которые могут быть улучшены. Мы представляем эти комментарии на рассмотрение GNSO.

Пояснение к рекомендации № 14:
Рекомендация № 14.8 ошибочна и, вероятно, в ней нет необходимости. Она гласит: «При внедрении и эксплуатации SSAD следует избегать непропорционально высокой нагрузки на небольших операторов». Мы не думаем, что кому-то известно, какой смысл у фразы «непропорционально высокая нагрузка на небольших операторов» или каковы последствия такой формулировки. Очевидно, что каждый регистратор и оператор регистратуры, независимо от их размера, будут обязаны использовать SSAD. Для ее использования любому «оператору» придется приложить минимально необходимое количество усилий. Это относится к стоимости ведения бизнеса в пространстве gTLD и сохранения аккредитации ICANN. Мы опасаемся, что пункт 14.8 будет использоваться как способ лишить SSAD необходимой функциональности.

Раздел «Руководство по реализации» в рекомендации № 14 также нуждается в соответствующем изменении.

Рекомендация № 18.2.3 гласит: «Чтобы отправить Совету GNSO официальные рекомендации по вопросам функционирования и политики SSAD, члены Постоянного комитета должны прийти к консенсусу по этим рекомендациям. Для достижения консенсуса по рекомендациям **потребуется поддержка сторон, связанных договорными обязательствами**». (выделение добавлено)

Постоянный комитет может дать два вида рекомендаций:

- Один из них — это рекомендации по внесению в договор изменений, имеющих юридическую силу. При голосовании в GNSO в соответствии с Уставом ICANN для них установлена высокая планка

(суперквалифицированное большинство). Для их принятия, по существу, требуется одобрение сторон, связанных договорными обязательствами.

- Другой вид — это рекомендации по реализации. Они не имеют юридической силы для сторон, связанных договорными обязательствами.

Проблема в том, что согласно рекомендации № 18 высокая планка суперквалифицированного большинства применяется в обоих случаях, но должна применяться только в первом случае. Рекомендация № 18 в ее текущей формулировке дает сторонам, связанным договорными обязательствами, право вето при выборе варианта реализации. Насколько нам известно, предоставление какой-либо стороне или палате права вето на решения такого уровня не является стандартным процессом принятия решений в GNSO.[151]

Существует также практическая проблема: мы не знаем, захотят ли SO и AC участвовать в работе Постоянного комитета, если один или два участника могут наложить вето на решения по вопросам реализации.

Мы не понимаем, как проблемы реализации могут подняться до уровня процесса получения руководящих указаний GNSO, который требует квалифицированного большинства голосов.

9 Благодарности, заявления о заинтересованности, возражения, альтернативные мнения и отказы от участия

В интересах транспарентности в этих разделах читателю предлагается информация о различных аспектах деятельности SSAC. В разделе «Благодарности» перечислены члены SSAC, сторонние эксперты и сотрудники ICANN, которые внесли непосредственный вклад в подготовку настоящего документа. В разделе «Заявления о заинтересованности» содержатся ссылки на биографии членов SSAC, где раскрываются любые интересы, способные стать источником конфликтов — фактических, кажущихся или потенциальных, — препятствующих участию этого члена комитета в подготовке настоящего отчета. Раздел «Возражения и альтернативные мнения» дает возможность отдельным членам описать причины своего несогласия с содержанием настоящего документа или процессом его подготовки, а также выразить альтернативное мнение. В разделе «Отказы от участия» указаны отдельные члены комитета, отказавшиеся от участия в обсуждении тем, затрагиваемых в настоящем отчете. Настоящий документ был единодушно одобрен всеми членами SSAC, кроме тех, которые перечислены в разделах «Возражения и альтернативные мнения» или «Отказы от участия».

[151] Мы не понимаем, как проблемы реализации могут подняться до уровня процесса получения руководящих указаний GNSO, который требует квалифицированного большинства голосов.

9.1 Благодарности

Комитет выражает свою благодарность следующим членам SSAC за потраченное время, усилия и анализ, выполненный при подготовке настоящего отчета.

Члены SSAC
Грег Аарон (Greg Aaron)
Бенедикт Аддис (Benedict Addis)
Бен Батлер (Ben Butler)
Стив Крокер (Steve Crocker)
Джеймс Гэлвин (James Galvin)
Джон Левин (John Levine)
Род Расмуссен (Rod Rasmussen)
Тара Уэйлен (Tara Whalen)

Персонал ICANN
Эндрю Макконахи (Andrew McConachie)
Даниэль Резерфорд (Danielle Rutherford)
Кэти Шнитт (Kathy Schnitt)
Стив Шенг (Steve Sheng, редактор)

9.2 Заявления о заинтересованности

Биографические сведения о членах SSAC и о сферах их интересов приведены здесь: https://www.icann.org/resources/pages/ssac-biographies-2019-11-20-en

9.3 Возражения и альтернативные мнения

Возражений или альтернативных мнений не поступило.

9.4 Отказы от участия

Отказов от участия не поступило.

Приложение F. Вклад сообщества

F.1. Запрос комментариев у SO/AC/SG/C

В соответствии с руководством по PDP GNSO, на раннем этапе своей деятельности Группа по EPDP была обязана направить каждой группе заинтересованных сторон и группе интересов GNSO официальные просьбы представить заявления. Группе по EPDP также рекомендовалось запросить мнение других организаций поддержки и консультативных комитетов ICANN, у которых могут быть знания, опыт или интерес к рассматриваемому вопросу. Как следствие, в начале обсуждения Группа по EPDP обратилась ко всем организациям поддержки и консультативным комитетам ICANN, а также к группам заинтересованных сторон и группам интересов GNSO с просьбой внести свой вклад на фазе 2. В ответ были получены заявления от следующих групп, комитетов и организаций:

- Группа интересов коммерческих пользователей GNSO (BC)
- Группа некоммерческих заинтересованных сторон GNSO (NCSG)
- Группа заинтересованных сторон-регистратур (RySG)
- Группа заинтересованных сторон-регистраторов (RrSG)
- Группа интересов интернет-провайдеров и провайдеров связи (ISPCP)

Полный текст заявлений находится здесь: https://community.icann.org/x/zIWGBg.

Все полученные комментарии были добавлены в инструмент анализа предварительных комментариев и изучены Группой по EPDP.

F.2. Форум общественного обсуждения первоначального отчета

7 ноября 2020 года Группа по EPDP опубликовала свой первоначальный отчет для общественного обсуждения. В первоначальном отчете были изложены основные вопросы, обсуждаемые в связи с предлагаемой Системой обеспечения стандартизованного доступа к закрытым регистрационным данным gTLD и их раскрытия (SSAD), а также предварительные рекомендации.

Для оптимизации анализа комментариев общественности Группа по EPDP воспользовалась формой Google. От групп заинтересованных сторон и групп интересов GNSO, консультативных комитетов ICANN, компаний и организаций поступило сорок пять комментариев помимо двух комментариев от частных лиц. С этими комментариями можно ознакомиться здесь: https://docs.google.com/spreadsheets/d/1EBiFCsWfqQnMxEcCaKQywCccEVdBc9_ktPA3PU8nrQk/edit?usp=sharing.

Для оптимизации рассмотрения результатов общественного обсуждения Группа по EPDP разработала комплект инструментов анализа комментариев общественности (PCRT) и таблицы обсуждений (см. https://community.icann.org/x/Hi6JBw). Используя онлайн-анализ и работая на пленарных заседаниях, Группа по EPDP выполнила анализ и оценку представленных комментариев и согласовала изменения рекомендаций и (или) отчета.

F.3. Общественное обсуждение дополнения к отчету

26 марта 2020 года Группа по EPDP опубликовала дополнение к первоначальному отчету для общественного обсуждения. Дополнение касается предварительных рекомендаций и выводов Группы по EPDP по указанным выше вопросам с приоритетом 2.

Для оптимизации анализа комментариев общественности Группа по EPDP воспользовалась формой Google. От групп заинтересованных сторон и групп интересов GNSO, консультативных комитетов ICANN, компаний и организаций поступило двадцать восемь комментариев помимо одного комментария от частного лица. С этими комментариями можно ознакомиться здесь: https://docs.google.com/spreadsheets/d/1jN5ThNtmcVJ8txdAGw0ynl5vrGJOuEv8xeccvzjR9qM/edit#gid=2086811131.

Для оптимизации рассмотрения результатов общественного обсуждения Группа по EPDP разработала комплект инструментов анализа комментариев общественности (PCRT) и таблицы обсуждений (см. https://community.icann.org/x/Hi6JBw). Используя онлайн-анализ и работая на пленарных заседаниях, Группа по EPDP выполнила анализ и оценку представленных комментариев и согласовала рекомендации по приоритету 2 и (или) выводы, которые следует включить в итоговый отчет.

Приложение G. Юридический комитет

Вопросы фазы 2, отправленные в Bird & Bird

1. Рассмотреть систему обеспечения стандартизованного доступа к закрытым регистрационным данным и их раскрытия, в которой:

    - Стороны, связанные с ICANN договорными обязательствами («CP»), обязаны раскрывать регистрационные данные, в том числе персональные данные.
    - Данные должны раскрываться подателям запросов через RDAP напрямую или через посреднический орган по аккредитации/авторизации запросов.
    - Аккредитация проводится третьей стороной по заказу ICANN без участия CP.
    - Данные раскрываются в автоматическом режиме без какого-либо ручного вмешательства.
    - Субъекты данных должным образом информируются в соответствии с контрактными требованиями ICANN о целях и типах организаций, которые могут обрабатывать персональные данные. Контракт CP с ICANN также требует, чтобы CP уведомляла субъекта данных о возможности такого раскрытия данных и их обработки третьими сторонами перед тем, как субъект данных заключит регистрационный договор с CP, а также ежегодно посредством отправки по предписанию ICANN напоминания о необходимости поддерживать точность регистрационных данных.
      CP соблюдают эти требования.

    Кроме того, предполагается, что внедрены следующие механизмы защиты

    - ICANN или ее уполномоченный проверили/подтвердили личность подателя запроса и в каждом случае потребовали, чтобы податель запроса:
        - заявлял, что у него есть законные основания для запроса и обработки данных;
        - представлял свое законное основание;
        - заявлял, что он запрашивает только данные, необходимые для его цели;
        - соглашался обрабатывать данные в соответствии с GDPR;
        - соглашался со стандартными договорными положениями ЕС о передаче данных.

    - ICANN или ее уполномоченный регистрирует запросы на получение закрытых регистрационных данных, регулярно проверяет эти журналы, принимает меры по обеспечению соблюдения нормативных требований при обнаружении признаков злоупотреблений и делает эти журналы доступными по запросу субъекта данных.

1. С каким риском или ответственностью, если таковые имеются, столкнется СР в связи с раскрытием данных в этом контексте, включая риск злоупотребления или обхода механизмов защиты третьей стороной?

2. Считаете ли вы изложенные выше критерии и механизмы защиты достаточными для того, чтобы раскрытие регистрационных данных соответствовало требованиям? Если существует какой-либо риск, какие улучшенные или дополнительные меры предосторожности устранят[1] этот риск?

3. В этом сценарии СР будет контролером или стороной, ответственной за обработку данных[2], и насколько это различие между контролером и стороной, ответственной за обработку данных, влияет на ответственность СР?

4. Отвечайте только в том случае, если риск для СР все еще существует: Если риск для СР все еще существует, какие дополнительные меры могут потребоваться для устранения ответственности СР в зависимости от характера запроса о раскрытии данных, то есть в зависимости от того, запрашиваются ли данные, например, негосударственными субъектами на основании гражданских исков или правоохранительными органами в зависимости от их юрисдикции или характера преступления (правонарушение или тяжкое преступление) или связанных с ним санкций (штраф, тюремное заключение или смертная казнь)?

Сноска 1: «Здесь важно подчеркнуть особую роль, которую механизмы защиты способны сыграть в уменьшении ненадлежащего воздействия на субъектов данных и, таким образом, в изменении баланса прав и интересов до такой степени, что законные интересы контролера данных не будут ущемлены». (https://iapp.org/media/pdf/resource_center/wp217_legitimate-interests_04-2014.pdf)

Сноска 2: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

2. В какой степени (если таковая имеется) стороны, связанные договорными обязательствами, несут ответственность за действия третьей стороны, получившей доступ к закрытым данным WHOIS в рамках схемы аккредитации, когда получившее доступ лицо аккредитовано для заявленной цели, обязуется принять определенные разумные меры предосторожности, аналогичные кодексу поведения в отношении использования данных, но искажает предполагаемые цели обработки таких данных и впоследствии обрабатывает их способом, несовместимым с заявленной целью. При таких обстоятельствах, если существует вероятность привлечения к ответственности сторон, связанных договорными

обязательствами, какие можно предпринять шаги, чтобы смягчить или уменьшить риск ответственности сторон, связанных договорными обязательствами?

3. Предполагая, что существует политика, которая позволяет аккредитованным сторонам получать доступ к закрытым данным WHOIS через SSAD (и требует от аккредитованной стороны принятия определенных разумных мер безопасности, аналогичных кодексу поведения), допустимо ли с точки зрения закона в соответствии со статьей 6(1)(f):

   · определить конкретные категории запросов от аккредитованных сторон (например, оперативное реагирование на атаку вредоносного ПО или установление связи с нарушителем прав на интеллектуальную собственность, не отвечающим на запросы), для которых может быть предусмотрена автоматическая отправка закрытых данных WHOIS без необходимости вручную проверять квалификацию аккредитованной стороны для каждого отдельного запроса о раскрытии, и (или)
   · обеспечить автоматическое раскрытие таких данных, не требуя ручного просмотра контролером или стороной, ответственной за обработку данных, каждого отдельного запроса о раскрытии.

Кроме того, если невозможно автоматизировать какой-либо из этих шагов, мы просим дать какие-либо инструкции по проверке баланса интересов в соответствии со статьей 6(1)(f).

Для справки см. следующие потенциальные механизмы защиты:

· Раскрытие информации требуется по контракту CP с ICANN (в соответствии с политикой фазы 2 EPDP).
· Контракт CP с ICANN требует, чтобы CP уведомляла субъекта данных о целях и типах организаций, которые могут обрабатывать персональные данные. CP должна уведомить об этом субъекта данных с возможностью отказа перед тем, как субъект данных заключит регистрационный договор с CP, а также ежегодно посредством отправки по предписанию ICANN напоминания о необходимости поддерживать точность регистрационных данных. CP соблюдают эти требования.

ICANN или ее уполномоченный проверили личность подателя запроса и потребовали, чтобы податель запроса:

- заявлял, что у него есть законные основания для запроса и обработки данных;
- представлял свое законное основание;
- заявлял, что он запрашивает только данные, необходимые для его цели;
- соглашался обрабатывать данные в соответствии с GDPR;

- соглашался со стандартными договорными положениями о передаче данных.

· ICANN или ее уполномоченный регистрирует запросы на получение закрытых регистрационных данных, регулярно проверяет эти журналы, принимает меры по обеспечению соблюдения нормативных требований при обнаружении признаков злоупотреблений и делает эти журналы доступными по запросу субъекта данных.

4. Согласно GDPR, контролер данных может раскрыть персональные данные правоохранительным/компетентным органам согласно ст. 6 1 с GDPR при условии, что правоохранительные органы имеют законные полномочия накладывать юридические обязательства в соответствии с действующим законодательством. Некоторые авторы комментариев интерпретировали «юридическое обязательство» как применимое только к юридическим обязательствам, основанным на законодательстве ЕС или государства-участника.

Что касается контролера данных:

а. Следует ли из этого, что контролер данных не может опираться на ст. 6 1 с GDPR при раскрытии персональных данных правоохранительным органам за пределами юрисдикции контролера данных? Как вариант, существуют ли обстоятельства, при которых контролеры данных могут опираться на ст. 6 1 с GDPR при раскрытии персональных данных правоохранительным органам за пределами юрисдикции контролера данных?

б. Может ли контролер данных опираться на любые другие правовые основы, помимо ст. 6 I f GDPR, для раскрытия персональных данных правоохранительным органам за пределами юрисдикции контролера данных?

Что касается правоохранительных органов:

Учитывая, что ст. 6 1 GDPR гласит, что европейские государственные органы не могут использовать ст. 6 I f GDPR в качестве правовой основы для обработки данных при выполнении своих задач, эти государственные органы должны иметь законное основание, чтобы раскрытие информации могло происходить на другой правовой основе (например, статья 6 I c GDPR).

с. В свете этого, могут ли правоохранительные органы за пределами ЕС опираться на ст. 6 I f GDPR как на правовую основу для обработки? В этом контексте, может ли контролер данных опираться на ст. 6 1 f GDPR при раскрытии персональных данных? Если правоохранительные органы за пределами ЕС не могут опираться на ст. 6 1 f GDPR в качестве правовой основы для обработки, на какое законное основание могут опираться правоохранительные органы за пределами ЕС?

- Основные положения[152]

Вопросы 1 и 2

Основные положения:
Группа по EPDP в рамках фазы 2 отправила Bird & Bird свой первый пакет вопросов 29 августа 2019 года. Bird & Bird ответила на этот пакет вопросов серией из трех меморандумов. Меморандум 1 доставлен 9 сентября 2019 года. В меморандуме 1 проанализирована правовая роль сторон, связанных договорными обязательствами, в предлагаемой Системе стандартизованного доступа к закрытым регистрационным данным и их раскрытия (SSAD), достаточность предлагаемых механизмов защиты и риск ответственности сторон, связанными договорными обязательствами, за раскрытие данных через SSAD. Вопросы, отправленные Bird & Bird, представлены в Приложении к настоящему документу и содержат ряд предположений в разделах 1.1 и 1.2, которые являются частью фактической основы для приведенных ниже ответов.

В ответ на эти вопросы Bird & Bird отметила следующее в отношении функции контролера данных:

1. Стороны, связанные договорными обязательствами, скорее всего, являются контролерами в SSAD, поскольку владельцы доменов обоснованно ожидают, что стороны, связанные договорными обязательствами, будут контролировать раскрытие их данных третьим сторонам. Трудно продемонстрировать, что стороны, связанные договорными обязательствами, служат только интересам корпорации ICANN, особенно в свете соответствующих судебных решений, которые предполагают низкий порог для контроля.
2. Если Группа по EPDP хотела бы рекомендовать политику, в соответствии с которой стороны, связанные договорными обязательствами, являются в SSAD сторонами, ответственными за обработку данных, можно было бы предпринять шаги для поддержки этой цели политики. Стороны, связанные договорными обязательствами, не должны иметь существенного влияния на ключевые аспекты обработки данных в SSAD, например (i) какие данные должны обрабатываться; (ii) как долго они будут обрабатываться; и (iii) кто должен иметь доступ к данным. Также возникнет необходимость в «постоянном и тщательном» надзоре со стороны корпорации ICANN «для обеспечения полного соблюдения стороной, ответственной за обработку данных, инструкций и условий контракта», а также в усилиях по информированию владельцев доменов о том, что стороны, связанные договорными обязательствами, действуют только от имени корпорации ICANN (например, материалы сайта корпорации ICANN, уведомления о

[152] Будет обновлено, когда Юридический комитет утвердит основные положения

конфиденциальности, предоставление информации в процессе регистрации доменного имени).

3. Однако наиболее вероятным исходом и исходной позицией для надзорных органов будет то, что стороны, связанные договорными обязательствами, являются контролерами и, вероятно, контролерами, совместно отвечающими за обработку данных с корпорацией ICANN в отношении раскрытия регистрационных данных через SSAD.

Bird & Bird отметила следующее в отношении механизмов защиты и ответственности SSAD:

4. Учитывая количество задействованных юрисдикций и вероятное разнообразие запросов, которые могла бы обрабатывать SSAD, Bird & Bird не смогла подтвердить, что благодаря критериям и механизмам защиты, описанным в предположениях, раскрытие данных в полностью автоматизированной SSAD будет соответствовать требованиям.
5. Bird & Bird предложила дополнительные механизмы защиты, которые следует рассмотреть в рамках EPDP, в отношении (i) законного основания, пропорциональности и минимизации данных; (ii) прав личности; (iii) международной передачи данных; и (iv) безопасности.
6. Согласно GDPR, стороны, участвующие в одной и той же обработке, несут ответственность как перед физическими лицами, так и перед надзорными органами. Индивидуальная ответственность является совместной и раздельной. Это означает, что каждая сторона, участвующая в обработке, потенциально несет ответственность за весь ущерб, нанесенный субъекту данных, с некоторыми различными нормами для контролеров и сторон, ответственных за обработку данных. Надзорные органы могут возбуждать уголовные дела против контролеров или сторон, ответственных за обработку данных, и в настоящее время неясно, применяется ли солидарная ответственность, когда несколько сторон участвуют в одной и той же обработке (то есть меры принуждения не подходят, если ответственность несут другие).

1. Являются ли стороны, связанные договорными обязательствами, контролерами или сторонами, ответственными за обработку данных?

Контролеры

- На ответственность существенно влияет то, являются ли стороны, связанные договорными обязательствами, контролерами или сторонами, ответственными за обработку данных. (1.4)

- Контролер — это физическое или юридическое лицо, государственный орган, агентство или другое учреждение, которое самостоятельно или вместе с другими лицами определяет цели и средства обработки персональных данных. (2.2)

- Является ли организация контролером – это фактическое определение, основанное на «контроле над ключевыми решениями по обработке данных». Роль контролера не может быть назначена и от нее нельзя отказаться. (2.3)

- Рабочая группа 29-й статьи представила руководство по функциям контролера и стороны, ответственной за обработку данных, действовавшее до GDPR. EDPB в настоящее время пересматривает это руководство; обновление ожидается в ближайшие шесть месяцев. (2.4, 2.19)

- Предшественник EDPB, Рабочая группа 29-й статьи (WP29), определила, что «первая и главная роль концепции контролера — это определение того, кто будет нести ответственность за соблюдение правил защиты данных и как субъекты данных могут осуществлять права на практике. Другими словами: распределение ответственности». Если понимать буквально, это означает, что контролер несет ответственность за большинство обязательств в соответствии с GDPR; но эта фраза также указывает на степень целесообразности регулирования: она указывает на основополагающую необходимость возложить на кого-то ответственность. По мнению B&B, это может повлиять на подход суда или надзорного органа. (2.4)

- Организация, которая принимает ключевые решения (самостоятельно или совместно с другими) относительно (i) того, какие данные обрабатываются; (ii) продолжительности обработки; и (iii) круга лиц, имеющих доступ к данным (их иногда называют «существенными элементами» обработки), действует как контролер, а не как сторона, ответственная за обработку данных. (2.6)

- Организация может быть как контролером, так и стороной, ответственной за обработку данных. Это бывает в том случае, когда организация, выступающая в качестве стороны, ответственной за обработку данных, также использует персональные данные в своих целях. (2.7)

Стороны, ответственные за обработку данных

- Сторона, ответственная за обработку данных — это «физическое или юридическое лицо, государственный орган, агентство или другой орган, который обрабатывает персональные данные от имени контролера». (2.5)

- Руководство Рабочей группы 29-й статьи подчеркивает важность изучения «степени фактического контроля, осуществляемого стороной, его модели, представленной субъектам данных, и разумных ожиданий субъектов данных на основе этого представления» при определении того, является ли организация контролером или стороной, ответственной за обработку данных. (2.5)
- Согласно WP29, сторона, ответственная за обработку данных, служит «чьим-то интересам», «выполняя полученные от контролера инструкции, по крайней мере, в отношении цели обработки и основных элементов средств». (2.5)

- Сторона, ответственная за обработку данных, может обрабатывать персональные данные только в соответствии с инструкциями контролера или в соответствии с требованиями законодательства ЕЭЗ или государства-участника. (2.7)

Применимость к SSAD

Презумпция контроля

- В некоторых случаях «существующие традиционные роли, которые обычно подразумевают определенную ответственность, помогут идентифицировать контролера: например, работодатель в отношении данных о своих сотрудниках, издатель в отношении данных о подписчиках, ассоциация в отношении данных о своих участниках или сотрудниках». Отношения между стороной, связанной договорными обязательствами, и владельцем домена (или контактным лицом владельца домена) можно рассматривать аналогичным образом. (2.8) Аналогичным образом, «модель, предоставляемая субъектам данных, и разумные ожидания субъектов данных» являются важным фактором при определении контроля. Владелец домена обычно ожидает, что стороны, связанные договорными обязательствами, будут контролировать раскрытие их данных третьим сторонам. (2.9)

- Поскольку стороны, связанные договорными обязательствами, в настоящее время рассматриваются как контролеры при раскрытии данных третьим сторонам, это приведет к презумпции того, что стороны, связанные договорными обязательствами, останутся контролерами даже после внедрения SSAD. (2.9)

- Однако такое предположение не всегда можно сделать в зависимости от анализа деятельности по технической обработке. WP169 отмечает, что при наличии предположения, что лицо является контролером (в WP169 это называется «контроль, проистекающий из неявной компетенции»), это должно иметь место

только «если другие элементы не указывают на обратное». Недавние дела CJEU — в частности, его недавнее постановление по Fashion ID — также подтверждают необходимость более тщательного анализа с учетом конкретных фактов. (2.11)

Сложность доказывания того, что стороны, связанные договорными обязательствами, действуют «от имени» кого-то другого

- Наиболее важным элементом роли стороны, ответственной за обработку данных, является то, что она действует только от имени контролера. Будет сложно продемонстрировать, что стороны, связанные договорными обязательствами, служат интересам ICANN и обрабатывают данные только от имени ICANN. (2.10)
- Раскрытие данных, вероятно, будет рассматриваться как неизбежное следствие статуса стороны, связанной договорными обязательствами, а не как согласие сторон, связанных договорными обязательствами, делать это от имени ICANN. (2.10)

Тщательный фактологический анализ деятельности по технической обработке

- Фактический порог для того, чтобы стать контролером (определение целей или средств обработки), низкий. Тест, согласно CJEU, заключается в том, что кто-то просто «оказывает влияние на обработку персональных данных в своих целях и (…) участвует, как следствие, в определении целей и средств этой обработки». (2.12)
- В постановлении CJEU по делу Jehovan Todistajat национальная общественная организация «Свидетели Иеговы» была охарактеризована как обладающая «общими знаниями», поощрявшая и координировавшая сбор данных членами сообщества (проповедниками, совершающими подомовой обход) на очень общем уровне. Но, тем не менее, было признано, что эта организация подпадает под определение контролера, совместно с этими членами сообщества отвечающего за обработку данных. В постановлении CJEU по делу Fashion ID оператору сайта было достаточно интегрировать код сайта с программным кодом платформы Facebook, чтобы этого оператора признали участником определения «средств» сбора данных Facebook и совместным контролером с Facebook. (2.14)
- Следовательно, суды и надзорные органы, скорее всего, сочтут, что сторона, связанная договорными обязательствами, участвует в определении средств обработки, возможно, просто путем внедрения SSAD и взаимодействия с этой системой. (2.14)

Факторы, которые могут служить обоснованием статуса стороны, ответственной за обработку данных

- Ключ к тому, чтобы избежать статуса контролера — демонстрация того, что вы не участвуете в определении «существенных элементов» обработки (2.6).

- Кроме того, мониторинг ICANN соблюдения контрактных требований о раскрытии данных может быть доказательством взаимоотношений между контролером и стороной, ответственной за обработку данных, поскольку «постоянный и тщательный надзор со стороны контролера для обеспечения полного соблюдения стороной, ответственной за обработку данных, инструкций и условий контракта указывает на то, что контролер по-прежнему полностью и единолично контролирует операции по обработке». (2.16)

- Принятие мер для четкого информирования субъектов данных о том, что данные собираются только от имени ICANN (например, раскрытие информации в процессе регистрации доменного имени, ежегодное напоминание о необходимости поддерживать точность данных, уведомления о конфиденциальности, материалы сайта корпорации ICANN) и предоставление других материалов, четко указывающих на то, что это действие выполняется СР исключительно от имени ICANN, могут привести к тому, что люди станут лучше осведомлены о роли ICANN как контролера и роли сторон, связанных договорными обязательствами, как сторон, ответственных за обработку данных. (2.17)

Резюме: стороны, связанные договорными обязательствами, скорее всего, являются контролерами, совместно отвечающими за обработку данных с ICANN

- Наиболее вероятным результатом и отправной точкой для надзорных органов будет то, что стороны, связанные договорными обязательствами, являются контролерами. (2.18)

- Роль ICANN в определении цели и средств обработки предполагает, что они являются контролерами, совместно отвечающими за обработку данных со сторонами, связанными договорными обязательствами, в отношении раскрытия данных третьим сторонам. (2.18)

2. Достаточно ли предложенных механизмов защиты для того, чтобы раскрытие регистрационных данных отвечало предъявляемым требованиям?

Механизмы защиты SSAD

- Учитывая количество задействованных юрисдикций и вероятное разнообразие запросов, которые могла бы обрабатывать SSAD, нельзя с уверенностью утверждать, что благодаря критериям и механизмам защиты, описанным в предположениях, раскрытие данных в полностью автоматизированной системе будет соответствовать требованиям. (3.8)

- B&B заявляет, что при обработке персональных данных необходимо проявлять осторожность — сторона, ответственная за обработку данных (либо в нарушение своего контракта с контролером, либо иным образом нарушает своими действиями инструкции контролера), может сама стать контролером и, таким

образом, столкнуться с нарушениями (как указано в таблице на стр. 7 меморандума). (3.6)

- Описанные механизмы защиты полезны, но они должны включать дополнительные меры, описанные ниже. (3.8)
    - Законное основание: механизмы защиты должны (i) учитывать, есть ли у сторон, связанных договорными обязательствами, а не только у подателя запроса, законное основание для обработки; (ii) учитывать конкретную правовую базу, применимую к стороне, связанной договорными обязательствами; (iii) обеспечить выполнение соответствующей проверки сбалансированности законных интересов, если это является надлежащим законным основанием в данном случае[153] (и может быть небезопасно предполагать, что для некоторой категории запросов баланс интересов всегда смещен в пользу раскрытия данных; определенные случаи, такие как расследования или судебное преследование, которые могут привести к смертной казни, могут быть особенно проблематичными); и (iv) гарантии того, что неподходящие типы или объемы данных не будут раскрыты подателям запросов (например, мониторинг на основе правил или блокирование запросов необычного размера, системы разрешений). (3.9 – 3.12)
    - Индивидуальные права: укажите, как обрабатываются запросы субъектов данных, включая (i) права доступа к журналам запросов (которые сами по себе могут относиться к персональным данным высокого риска или даже к персональным данным «особой категории»); (ii) соответствующий срок хранения этих журналов; (iii) способ предоставления информации субъектам данных; (iv) как поступать в ситуациях, когда податель запроса настаивает на том, чтобы не предоставлять информацию субъекту данных (например, конфиденциальность правоохранительных органов); и (v) запросы на ограничение или блокировку обработки. (3.13 – 3.16)
    - Передача данных: для международной передачи данных Группа по EPDP предусматривает использование в качестве механизма правовой защиты Стандартных договорных положений ЕС (SCC), однако (i) некоторые податели запросов, в том числе государственные органы, не согласятся с их условиями; (ii) условия SCC нелегко соблюдать, особенно в больших масштабах; (iii) если стороны, связанные договорными обязательствами, из ЕЭЗ являются сторонами, ответственными за обработку данных, они не могут напрямую опираться на SCC для передачи данных корпорации ICANN или подателям запросов за пределами ЕЭЗ, поэтому потребуется найти обходной путь. (3.17)

[153] Если раскрытие данных является юридическим обязательством согласно законам ЕС или государств-членов ЕС / ЕЭЗ (включая договоры, участником которых является ЕС или соответствующее государство-член), нет необходимости оценивать наличие законных интересов.

- Безопасность: механизмы защиты должны быть пропорциональны риску для субъектов данных, если их данные будут скомпрометированы. (3.18)

3. Каков риск ответственности сторон, связанных договорными обязательствами, за раскрытие данных?

- Если механизмы защиты неадекватны, либо если податели запросов злоупотребляют ими или обходят их (или нарушаются другие аспекты GDPR, например неадекватное уведомление или отсутствие законного основания для обработки), стороны, связанные договорными обязательствами, могут столкнуться с расследованиями, судебными постановлениями (например, запреты на обработку) и понести (материальную) ответственность как перед физическими лицами (гражданская), так и перед надзорными органами (штрафы).

- В общих чертах, B&B предлагает в соответствующих частях следующее: (1) если стороны являются контролерами, совместно отвечающими за обработку данных, это не означает, что каждая из сторон должна взять на себя все элементы соответствия требованиям, (2) если СР являются сторонами, ответственными за обработку данных, они будут нести ответственность только перед физическими лицами (гражданская ответственность) по ст. 82, если они не выполнили обязательства, возложенные в соответствии с Регламентом на сторон, ответственных за обработку данных, или действовали вне или вопреки законным инструкциям контролера, (3) даже если стороны считаются контролерами, совместно отвечающими за обработку данных, недавние судебные решения (о мерах принуждения со стороны надзорных органов) подчеркнули, что совместный контроль не подразумевает равную ответственность за нарушения GDPR, и (4) СР, как контролеры, совместно отвечающие за обработку данных с корпорацией ICANN, выиграют от четкого распределения ответственности в соответствии с условиями «соглашения» о совместном контроле, которое они должны заключить в соответствии со ст. 26.

Ответственность перед физическими лицами

- Статья 82 GDPR устанавливает правила ответственности перед физическими лицами. (4.2)

- Контролеры несут ответственность за ущерб, причиненный обработкой, нарушающей GDPR. Стороны, ответственные за обработку данных, несут ответственность за убытки, вызванные обработкой, когда такая сторона не выполнила предъявляемых к ней требований или когда она действовала вне или вопреки инструкциям контролера. (4.2)

- Контроллер или сторона, ответственная за обработку данных, не несет ответственность, если докажет, что никоим образом не отвечает за событие, повлекшее за собой ущерб. (4.2)

- Если несколько контролеров или сторон, ответственных за обработку данных, участвуют в одной и той же обработке, каждая организация несет ответственность за весь ущерб (солидарную ответственность) физическим лицам (4.2, 4.3).

- Если стороны, связанные договорными обязательствами, являются сторонами, ответственными за обработку данных, они несут ответственность только в том случае, если не соблюдают свои конкретные обязательства в соответствии с GDPR или действуют вне или вопреки инструкциям контролера. В таком сценарии маловероятно, что стороны, связанные договорными обязательствами, нарушат инструкции контролера, поскольку SSAD автоматизирована; поэтому более вероятным источником ответственности для них может быть ненадлежащие меры безопасности или несоблюдение правил GDPR в отношении международной передачи данных. Стороны, связанные договорными обязательствами, могут обратиться к корпорации ICANN с просьбой предписать меры безопасности и международной передачи, чтобы у этих сторон появилась возможность утверждать, что они «никоим образом не отвечают за событие, повлекшее за собой ущерб». (4.4)

- Если стороны, связанные договорными обязательствами, являются контролерами, и если раскрытие информации нарушает GDPR, они вряд ли смогут избежать ответственности перед физическими лицами, если не сумеют доказать, что «никоим образом не отвечают за событие, повлекшее за собой ущерб», если они активно участвуют в раскрытии данных.

- Любая ответственность создает возможность того, что стороны, связанные договорными обязательствами, будут нести ответственность за весь ущерб, причиненный субъекту данных. Этот риск является самым высоким при сценарии совместного контроля. (4.5, 4.6).

- Стороны, связанные договорными обязательствами, несущие ответственность за весь ущерб, нанесенный субъекту данных, могут требовать соответствующих вкладов со стороны других ответственных сторон. (4.7)

- Как контролеры, стороны, связанные договорными обязательствами, и ICANN будут иметь позитивное обязательство устранять риск того, что податели запросов попытаются получить неправомерный доступ к персональным данным. Механизмы защиты должны соответствовать уровню риска. Если податель запроса обходит механизмы защиты SSAD, суды могут признать эти механизмы адекватными, что ограничит основную ответственность сторон, связанных договорными обязательствами. (4.9, 4.10)

- Даже в случае нарушения GDPR по вине подателя запроса, стороны, связанные договорными обязательствами, ICANN и податель запроса могут считаться «вовлеченными в одну и ту же обработку», при этом каждая сторона несет солидарную ответственность за ущерб, возникший в результате этого нарушения. Сторонам, связанным договорными обязательствами, и ICANN возможно удастся доказать, что они «никоим образом не отвечают за событие, повлекшее за собой ущерб», но в противном случае им придется потребовать возмещения от подателя запроса или присоединиться к подателю запроса в первичных разбирательствах, чтобы распределить убытки. (4.11)

Ответственность перед надзорными органами

- Надзорные органы могут возбуждать дела против контролеров или сторон, ответственных за обработку данных. (4.12)

- Неясно, применяется ли солидарная ответственность, когда в обработке участвует несколько сторон (например, правоприменительные меры, возможно, неуместны, если ответственность несут другие). (4.13)

- В законе должна быть четкая формулировка, устанавливающая солидарную ответственность — это усилило бы аргумент, что об этом было прямо заявлено, если бы речь шла о штрафах со стороны надзорных органов. Ст. 83(2)(d) поясняет, что солидарная ответственность не применяется в отношении надзорных органов. (4.13.2)

- Даже когда стороны являются контролерами, совместно отвечающими за обработку данных, в недавних судебных решениях (о мерах принуждения со стороны надзорных органов) подчеркивается, что совместный контроль не подразумевает равную ответственность за нарушения GDPR. (4.13.4)

- Таким образом, стороны, связанные договорными обязательствами, и ICANN получат выгоду от четко распределенных обязанностей в рамках соглашения о совместном контроле (и соглашение о совместном контроле в любом случае является обязательным во всех ситуациях совместного контроля в соответствии со статьей 26 GDPR). (4.14)

- Возможно, удастся воспользоваться положениями GDPR о «руководящем органе» (также известном как «единое окно» или «согласованность»), чтобы гарантировать осуществление всех правоприменительных действий через брюссельское отделение корпорации ICANN, а не против сторон, связанных договорными обязательствами. Этот механизм доступен только при трансграничной обработке персональных данных (организации в нескольких государствах-членах ЕЭЗ или влияние на субъектов данных в нескольких государствах-членах ЕЭЗ). (4.15 – 4.17)

- Положения о «руководящем органе» в GDPR не уделяют непосредственного внимания совместному контролю, но руководящие указания предполагают, что,

если корпорация ICANN и стороны, связанные договорными обязательствами, назначат бельгийское подразделение ICANN основным учреждением для обработки данных (то есть местом, где принимаются решения относительно обработки), это может свести к минимуму риск правоприменительных мер непосредственно в отношении сторон, связанных договорными обязательствами. Это новый и непроверенный подход. (4.15 – 4.20)

Приложение:
Правовые вопросы 1 и 2: ответственность, механизмы защиты, контролер и сторона, ответственная за обработку данных

Когда Группа по EPDP обсуждала архитектуру SSAD, возникло несколько вопросов, касающихся ответственности и механизмов защиты. В свою очередь, Юридический комитет фазы 2 сформулировал следующие вопросы внешнему юрисконсульту:

1. Рассмотреть систему обеспечения стандартизованного доступа к закрытым регистрационным данным и их раскрытия, в которой:

- Стороны, связанные с ICANN договорными обязательствами («СР»), обязаны раскрывать регистрационные данные, в том числе персональные данные.
- Данные должны раскрываться подателям запросов через RDAP напрямую или через посреднический орган по аккредитации/авторизации запросов.
- Аккредитация проводится третьей стороной по заказу ICANN без участия СР.
- Данные раскрываются в автоматическом режиме без какого-либо ручного вмешательства.
- Субъекты данных должным образом информируются в соответствии с контрактными требованиями ICANN о целях и типах организаций, которые могут обрабатывать персональные данные. Контракт СР с ICANN также требует, чтобы СР уведомляла субъекта данных о возможности такого раскрытия данных и их обработки третьими сторонами перед тем, как субъект данных заключит регистрационный договор с СР, а также ежегодно посредством отправки по предписанию ICANN напоминания о необходимости поддерживать точность регистрационных данных.
  СР соблюдают эти требования.

Кроме того, предполагается, что внедрены следующие механизмы защиты

- ICANN или ее уполномоченный проверили/подтвердили личность подателя запроса и в каждом случае потребовали, чтобы податель запроса:
  - заявлял, что у него есть законные основания для запроса и обработки данных;
  - представлял свое законное основание;
  - заявлял, что он запрашивает только данные, необходимые для его цели;
  - соглашался обрабатывать данные в соответствии с GDPR;
  - соглашался со стандартными договорными положениями ЕС о передаче данных.
- ICANN или ее уполномоченный регистрирует запросы на получение закрытых регистрационных данных, регулярно проверяет эти журналы, принимает меры по обеспечению соблюдения нормативных требований при обнаружении признаков злоупотреблений и делает эти журналы доступными по запросу субъекта данных.

a. С каким риском или ответственностью, если таковые имеются, столкнется СР в связи с раскрытием данных в этом контексте, включая риск злоупотребления или обхода механизмов защиты третьей стороной?

b. Считаете ли вы изложенные выше критерии и механизмы защиты достаточными для того, чтобы раскрытие регистрационных данных соответствовало требованиям? Если существует какой-либо риск, какие улучшенные или дополнительные меры предосторожности устранят[154] 1 этот риск?

c. В этом сценарии СР будет контролером или стороной, ответственной за обработку данных[155] 2, и насколько это различие между контролером и стороной, ответственной за обработку данных, влияет на ответственность СР?

d. Отвечайте только в том случае, если риск для СР все еще существует:
Если риск для СР все еще существует, какие дополнительные меры могут потребоваться для устранения ответственности СР в зависимости от характера запроса о раскрытии данных, то есть в зависимости от того, запрашиваются ли данные, например, негосударственными субъектами на основании гражданских

[154] «Здесь важно подчеркнуть особую роль, которую механизмы защиты способны сыграть в уменьшении ненадлежащего воздействия на субъектов данных и, таким образом, в изменении баланса прав и интересов до такой степени, что законные интересы контролера данных не будут ущемлены». (https://iapp.org/media/pdf/resource_center/wp217_legitimate-interests_04-2014.pdf)

[155] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

исков или правоохранительными органами в зависимости от их юрисдикции или характера преступления (правонарушение или тяжкое преступление) или связанных с ним санкций (штраф, тюремное заключение или смертная казнь)?

2. В какой степени (если таковая имеется) стороны, связанные договорными обязательствами, несут ответственность за действия третьей стороны, получившей доступ к закрытым данным WHOIS в рамках схемы аккредитации, когда получившее доступ лицо аккредитовано для заявленной цели, обязуется принять определенные разумные меры предосторожности, аналогичные кодексу поведения в отношении использования данных, но искажает предполагаемые цели обработки таких данных и впоследствии обрабатывает их способом, несовместимым с заявленной целью. При таких обстоятельствах, если существует вероятность привлечения к ответственности сторон, связанных договорными обязательствами, какие можно предпринять шаги, чтобы смягчить или уменьшить риск ответственности сторон, связанных договорными обязательствами?

Вопрос 3

Основные положения:

Группа по EPDP в рамках фазы 2 отправила Bird & Bird свой первый пакет вопросов 29 августа 2019 года. Bird & Bird ответила на этот пакет вопросов серией из трех меморандумов. Меморандум 2 был представлен 10 сентября 2019 года; в нем проанализированы вопросы, связанные с тем, как «проверка сбалансированности» законных интересов, требуемая в соответствии со статьей 6(1)(f) GDPR, может быть применена в SSAD с высокой степенью автоматизации (вопрос A), либо, если невозможно автоматизировать такое решение, как следует проводить проверку сбалансированности (вопрос B). Полный перечень вопросов представлен в Приложении A к настоящему резюме и включает ряд предположений, которые являются частью фактологической основы для приведенных ниже ответов.

В ответ на вопрос A компания Bird & Bird отметила следующее в отношении функции автоматизации:

1. Высокоавтоматизированный процесс, описанный Группой по EPDP, можно приравнять к исключительно автоматизированному принятию решений, оказывающих юридическое или аналогичное существенное влияние на субъектов данных («субъектами данных» в данном случае являются объекты запроса закрытых регистрационных данных gTLD).
2. Как правило, это не допускается, если только одно из ограниченных правовых оснований/исключений в соответствии со ст. 22(1) GDPR не оправдывает раскрытие данных. Это намного уже, чем GDPR Ст. 6(1)(f). Предлагаемой SSAD будет сложно выполнить требование GDPR ст. 22(1) в отношении исключений; поэтому структура SSAD должна быть такой, чтобы она вообще не подпадала под действие статьи 22.
3. Для этого необходимо ограничить автоматический доступ к данным и их раскрытие только теми случаями, когда нет «юридических или аналогичных значимых последствий» для субъекта данных. Примеры, представленные в меморандуме, включают раскрытие контактных данных администратора у владельцев доменов, не являющихся физическими лицами, в ответ на атаки вредоносного ПО или нарушение прав на интеллектуальную собственность. Процесс обработки запросов с повышенным риском не должен быть полностью автоматизирован; должно быть какое-то значимое человеческое участие (по крайней мере, надзор).
4. В качестве альтернативы SSAD может быть структурирована так, чтобы она не принимала решения на основе автоматической обработки персональных данных, относящихся к объектам запроса. Например, SSAD могла бы публиковать категории допустимых запросов и запрашивать у подателей запросов подтверждение того, что они соответствуют установленным критериям. За счет такого обратного требования к *подателю запроса* провести необходимый анализ и затем

подтвердить результат для SSAD, вероятно, SSAD не будет считаться системой, принимающей решение (о раскрытии данных) на основе собственной автоматизированной обработки персональных данных, и поэтому GDPR ст. 22 не будет применяться. Однако использование самосертификации подателями запросов, возможно, создает поле для злоупотреблений системой со стороны подателей запросов, что (как объяснялось в предыдущих ответах) может означать ответственность для ICANN и сторон, связанных договорными обязательствами.

5. Что касается аутентификации подателя запроса (в качестве шага, отдельного от оценки оснований или других параметров запроса), Bird & Bird считает, что процесс аутентификации лица, отправляющего запрос, безусловно, можно автоматизировать. Также возможно автоматизировать другие аспекты процесса запроса.

В ответ на вопрос B Bird & Bird:

1. Процитировала официальные руководящие указания ЕС (WP29) о том, как должна проводиться проверка сбалансированности законных интересов (ст. 6(1)(f)).
2. Отметила, что если ICANN и стороны, связанные договорными обязательствами, являются контролерами, совместно отвечающими за обработку данных, они оба должны заявить о законном интересе в обработке. Что касается сторон, связанных договорными обязательствами, вполне вероятно, что соответствующий интерес будет у третьей стороны — подателя запроса. ICANN, напротив, может заявить о своей заинтересованности в безопасности, стабильности и отказоустойчивости системы доменных имен, *равно как и в* удовлетворении интересов третьей стороны, подателя запроса.
3. Представила общее описание механизмов защиты, которые могут быть применены, чтобы еще больше склонить чашу весов в пользу обработки, предусмотренной в рамках SSAD.

1. Вопрос A

Вопрос A: позволяет ли статья 6(1)(f) GDPR (правовое основание для обработки: «законные интересы») автоматически обрабатывать в SSAD запросы (по крайней мере, в некоторых заранее определенных категориях) без необходимости вручную, запрос за запросом, (i) проверять, что запрос отвечает соответствующим критериям раскрытия данных, и (ii) раскрывать соответствующие регистрационные данные.

SSAD может подпадать под действие ст. 22 GDPR, а не только ст. 6(1)(f).

- GDPR ст. 6(1)(f) разрешает автоматизированную обработку *за исключением случаев*, когда это будет означать «автоматизированное индивидуальное принятие решений», имеющее юридические или аналогичные значимые последствия для субъекта данных («исключительно автоматизированное принятие решений»), что,

как правило, не допускается, если только одно из более ограниченных правовых оснований/исключений в соответствии со ст. 22(1) GDPR не оправдывает раскрытие данных.

- В то время как статья 22 GDPR гласит, что субъект данных имеет «право не подвергаться» такому решению, на практике статья 22 интерпретируется регулирующими органами как общий *запрет* (то есть субъекту данных нет необходимости возражать против такого принятия решения).

- Описанный Группой по EPDP процесс может сводиться к такому автоматизированному принятию решений, влияющему на объект запроса (например, когда правоохранительные органы хотят привлечь к ответственности лиц, использующих незаконные сайты).

- Если статья 22 применяется к обработке, описанной в EPDP, то есть **если обработка в SSAD представляет собой автоматизированное индивидуальное решение, имеющее юридические или аналогичные значимые последствия, это не будет разрешено в соответствии со ст. 6(1)(f) GDPR (основание для обработки: «законные интересы»).** Ст. 22 (1) устанавливает собственный, более ограниченный набор оснований, на которых могут приниматься решения по ст. 22.

- B&B сообщает, что в **SSAD будет сложно выполнить условия для освобождения от обязательств, указанные в ст. 22 (1); таким образом, EPDP должен гарантировать, что обработка SSAD не подпадает под действие ст. 22.**

Стратегия смягчения последствий 1: избегать решений, которые могут иметь «юридические или аналогичные значимые последствия» для лиц, данные которых раскрываются.

- Одним из способов достижения этого может быть ограничение автоматического доступа к данным и их раскрытия ситуациями, когда не будет «юридических или аналогичных значительных последствий» для субъекта данных.

- Решение о раскрытии данных через SSAD само по себе не будет иметь «юридических последствий» для субъекта данных. Более подходящий тест для SSAD — «аналогичные значимые последствия». Это означает нечто подобное юридическим последствиям — нечто заслуживающее внимания (например, существенное влияние на обстоятельства, поведение или выбор соответствующих лиц).[156]

- Возможно, удастся определить категории запросов, которые не имеют «юридических или аналогичных значимых» последствий для человека, например, раскрытие контактных данных администратора у лиц, не являющихся физическими

[156] Согласно официальному руководству, ниже приведены классические примеры решений, которые могут быть достаточно значимыми: (i) решения, влияющие на чье-либо финансовое положение; (ii) решения, влияющие на доступ к медицинским услугам; (iii) решения, которые лишают возможности трудоустройства или ставят кого-либо в серьезное невыгодное положение; (iv) решения, влияющие на чей-либо доступ к образованию.

(компания/организация/учреждение). Другое раскрытие данных о владельце домена-физическом лице может с гораздо большей вероятностью иметь «аналогичные значимые последствия». Такой анализ потребует серьезного внимания.

- Для принятия решений, которые с большей вероятностью будут иметь «значимые последствия», потребуется контроль или надзор со стороны человека. «Символического» человеческого участия было бы недостаточно. Чтобы элемент проверки со стороны человека был засчитан, контролер должен обеспечить значимый надзор со стороны того, кто имеет полномочия и компетенцию для изменения решения.

Стратегия смягчения последствий 2: Избегать реализаций SSAD, которые предусматривают обработку персональных данных об объекте запроса при принятии решения о том, выполнять ли запрос.

- Также можно структурировать SSAD таким образом, чтобы она не требовала «принятия решения исключительно на основании автоматизированной обработки». Статья 22 GDPR требует, чтобы решение основывалось на обработке *персональных данных.* Если решения основаны на чем-то другом, кроме персональных данных, статья 22 GDPR не применяется.

- Таким образом, вместо того, чтобы SSAD запрашивала детали у подателей запросов (например, информацию об объекте запроса, скажем, о владельце домена, и почему требуются его данные), а затем анализировала эту информацию (автоматически), чтобы оценить, соблюдаются ли установленные критерии разглашения закрытых регистрационных данных, SSAD может публиковать категории допустимых запросов и запрашивать у подателей запросов подтверждение того, что они соответствуют установленным критериям. В этом случае SSAD не будет обрабатывать *персональные данные* об объекте запроса, чтобы принять решение о раскрытии данных, и поэтому статья 22 не будет применяться.

- Как отмечалось в ответах на предыдущие вопросы, стороны, участвующие в SSAD, несут ответственность за принятие «соответствующих технических и организационных мер» для защиты от риска неправильного использования системы SSAD подателями запросов.

- Поэтому любое решение, основанное на самосертификации, а не на оценке запросов, должно быть тщательно сбалансировано с этими обязательствами по снижению рисков; это, вероятно, сократит количество случаев, когда можно использовать такой подход на основе собственных заявлений подателей запросов. Bird & Bird отмечает, что при такой схеме SSAD тем не менее может предлагать подателям запросов предоставить дополнительную информацию о характере их

запроса *для целей аудита*, но она не будет использоваться для оценки самого запроса (то есть не будет использоваться для автоматического принятия решений).

2. Вопрос B

В этом вопросе **Группа по EPDP просит дать рекомендации о том, как проверять сбалансированность интересов в соответствии с 6(1)(f) (при условии, что невозможно автоматизировать описанные шаги).**

- Официальное руководство гласит, что тест на сбалансированность интересов следует разделить на четыре этапа:

    1. Оценить интерес, которому отвечает обработка
    2. Учесть влияние на субъекта данных
    3. Провести предварительную проверку сбалансированности
    4. Учесть влияние всех дополнительных мер безопасности, принятых для предотвращения любого ненадлежащего воздействия на субъект данных.

1. Оценка законного интереса контролера

- В пункте 6(1)(f) сказано, что можно осуществлять законную обработку, если это «необходимо для удовлетворения законных интересов контролера или третьей стороны».

- Здесь есть три вложенных элемента: (i) легитимность; (ii) наличие интереса; и (iii) необходимость.

Легитимность

- Похоже, что «легитимность» не является строгой проверкой — по мнению WP29, «интерес может считаться законным, если контролер может проявлять этот интерес в соответствии с законодательством о защите данных и другими законами».

Обоснование наличия «интереса» в обработке

- B&B отметила, что если ICANN и стороны, связанные договорными обязательствами, являются контролерами, совместно отвечающими за обработку данных, они оба должны заявить о законном интересе в обработке. Что касается сторон, связанных договорными обязательствами, вполне вероятно, что соответствующий интерес будет у третьей стороны — подателя запроса. ICANN, напротив, может заявить о своей заинтересованности в безопасности, стабильности и отказоустойчивости системы доменных имен, равно как и в удовлетворении интересов третьей стороны, подателя запроса.

- «Интерес» и «цель» — это не одно и то же.
    - «Цель»: конкретная причина обработки данных.
    - «Интерес»: более широкая заинтересованность контролера в обработке, или выгода, которую извлекает контролер или может извлечь общество из обработки. (Это также означает, что интересы могут быть общественными или частными; например, в случае мер по предотвращению нарушения прав на товарный знак может быть частный интерес у владельца этого товарного знака, и более широкий общественный интерес в предотвращении риска введения пользователей в заблуждение. Этот фактор можно было бы указать в документации по проверке сбалансированности интересов.)
- Интерес должен быть «реальным и конкретным», а не «расплывчатым и спекулятивным».
- На стр. 25 в документе WP217 представлен неисчерпывающий список ситуаций, в которых могут возникать законные интересы, включая:
    - «Осуществление права на свободу слова или информации, в том числе в средствах массовой информации и в искусстве»
    - Удовлетворение законных требований
    - Предупреждение мошенничества и злонамеренного использования услуг
    - Физическая безопасность, ИТ и сетевая безопасность
    - Обработка в исследовательских целях
- Группа по EPDP предполагает, что потенциальные механизмы защиты SSAD моли бы включать требование к подателю запроса подтвердить, что у него есть законное основание для подачи запроса и он может «представить свое законное основание». Однако, если данные будут раскрываться в соответствии со статьей 6(1)(f), гораздо полезнее, чтобы податель запроса подтверждал свой *интерес* в получении персональных данных.

Необходимость

- Что касается необходимости, B&B сообщает, что предлагаемая обработка (раскрытие данных) должна быть «необходимой» для этих целей.
    - CEJU в рамках дела Oesterreichischer Rundfunk определяет это следующим образом: *«…прилагательное «необходимый»… подразумевает, что речь идет о «насущной общественной потребности» и что применяемая мера «соразмерна преследуемой законной цели»».*

- Апелляционный суд Великобритании также полагает, что «необходимое» означает «более чем желательное, но менее чем жизненно важное или абсолютно необходимое».

- B&B предполагает, что важным фактором, который следует учитывать при оценке необходимости, может быть факт попытки подателя запроса связаться с человеком каким-либо другим способом (хотя это может быть неуместным в случае запросов правоохранительных органов).

- B&B отмечает, что в SSAD предлагается требовать от подателей запросов подтверждения того, что запрашиваются только те данные, которые необходимы для их цели.

2. Оценка воздействия на человека

- B&B сообщает о том, что EDPB предлагает целый ряд факторов, которые следует учитывать при оценке воздействия на человека:

  - ***Оценка воздействия.*** Учитывайте прямое влияние на субъект данных, а также любые возможные более широкие последствия обработки данных (например, инициирование судебного разбирательства).

  - ***Характер данных.*** Учитывайте степень конфиденциальности данных, а также опубликованы ли они на данный момент.

  - ***Статус субъекта данных***. Учитывайте, повышает ли статус субъекта данных его уязвимость (например, дети, другие защищенные категории)

  - ***Объем обработки.*** Учитывайте, будут ли данные надежно храниться (меньший риск) по сравнению с публичным раскрытием, доступностью более широкой аудитории или объединением с другими данными (более высокий риск).

  - ***Разумные ожидания субъекта данных***. Учитывайте, будет ли субъект данных ожидать на разумных основаниях обработки/раскрытия его данных таким способом.

  - ***Статус контролера и субъекта данных.*** Учитывайте переговорные возможности и любые диспропорции в полномочиях контролера и субъекта данных.

- SSAD может принять во внимание эти факторы, определив запросы, которые могут представлять высокий риск для отдельных лиц, чтобы этим запросам уделялось дополнительное внимание.

- При оценке риска можно использовать классическую методологию управления рисками (анализ серьезности и вероятности).

- Это не является чисто количественной задачей; хотя показатели запроса (например, количество затронутых субъектов данных) актуальны, они не являются определяющими — все же следует учитывать потенциально значимое влияние на одного субъекта данных.

3. Предварительный баланс

- Как только законные интересы контролера или третьей стороны и интересы физического лица будут учтены, их можно сбалансировать. Гарантии выполнения других обязательств по защите данных помогают в обеспечении баланса, но не являются определяющими (например, SSAD, обеспечивающая наличие в договорах с подателями запросов стандартных положений об адекватной защите данных, полезна, поскольку это, возможно, снижает риск для физических лиц, но не является определяющим фактором).

4. Дополнительные механизмы защиты

- B&B сообщает, что если неясно, как достичь баланса, контролер может рассмотреть дополнительные меры предосторожности, чтобы снизить влияние обработки на субъектов данных.
- К ним относятся, например:
    - Транспарентность
    - Расширенные права субъектов на доступ или перенос данных
    - Безусловное право отказаться
- В документе WP217 на стр. 41–42 содержится более подробная информацию о мерах предосторожности, которые могут помочь «склонить чашу весов» в пользу обработки (в данном случае в пользу раскрытия данных) в законных интересах.

Приложение: Правовой вопрос 3: законные интересы и автоматизированная отправка и (или) раскрытие данных

a) Предполагая, что существует политика, которая позволяет аккредитованным сторонам получать доступ к закрытым данным WHOIS через систему обеспечения стандартизованного доступа к закрытым регистрационным данным и их раскрытия третьим лицам (SSAD) (и требует от аккредитованной стороны принятия определенных разумных мер безопасности, аналогичных кодексу поведения), допустимо ли с точки зрения закона в соответствии со статьей 6(1)(f):

- определить конкретные категории запросов от аккредитованных сторон (например, оперативное реагирование на атаку вредоносного ПО или установление связи с нарушителем прав на интеллектуальную собственность, не отвечающим на запросы), для которых может быть предусмотрена автоматическая отправка закрытых данных WHOIS без необходимости вручную проверять квалификацию аккредитованной стороны для каждого отдельного запроса о раскрытии, и (или)

- обеспечить автоматическое раскрытие таких данных, не требуя ручного просмотра контролером или стороной, ответственной за обработку данных, каждого отдельного запроса о раскрытии.

b) Кроме того, если невозможно автоматизировать какой-либо из этих шагов, мы просим дать какие-либо инструкции по проверке баланса интересов в соответствии со статьей 6(1)(f).

Для справки см. следующие потенциальные механизмы защиты:

- Раскрытие информации требуется по контракту CP с ICANN (в соответствии с политикой фазы 2 EPDP).
- Контракт CP с ICANN требует, чтобы CP уведомляла субъекта данных о целях и типах организаций, которые могут обрабатывать персональные данные. CP должна уведомить об этом субъекта данных с возможностью отказа перед тем, как субъект данных заключит регистрационный договор с CP, а также ежегодно посредством отправки по предписанию ICANN напоминания о необходимости поддерживать точность регистрационных данных. CP соблюдают эти требования.
- ICANN или ее уполномоченный проверили личность подателя запроса и потребовали, чтобы податель запроса:
  - заявлял, что у него есть законные основания для запроса и обработки данных;
  - представлял свое законное основание;
  - заявлял, что он запрашивает только данные, необходимые для его цели;

- соглашался обрабатывать данные в соответствии с GDPR;
- соглашался со стандартными договорными положениями о передаче данных.

- ICANN или ее уполномоченный регистрирует запросы на получение закрытых регистрационных данных, регулярно проверяет эти журналы, принимает меры по обеспечению соблюдения нормативных требований при обнаружении признаков злоупотреблений и делает эти журналы доступными по запросу субъекта данных.

Вопрос 4

Основные положения:
Группа по EPDP в рамках фазы 2 отправила Bird & Bird свой первый пакет вопросов 29 августа 2019 года. Bird & Bird ответила на этот пакет вопросов серией из трех меморандумов. Меморандум 3 был доставлен 9 сентября 2019 года и анализирует вопросы о законных основаниях, позволяющих раскрыть персональные данные, содержащиеся в регистрационных данных gTLD, правоохранительным органам за пределами юрисдикции контролера данных.

В частности, меморандум отвечает на следующие вопросы:

- Может ли контролер данных опираться на статью 6(1)(c) GDPR для раскрытия персональных данных правоохранительным органам за пределами юрисдикции контролера данных?
- Если нет, может ли оператор данных опираться на любые другие правовые основания, помимо статьи 6(1)(f), для раскрытия персональных данных правоохранительным органам за пределами юрисдикции контролера данных?
- Могут ли правоохранительные органы за пределами ЕС опираться на ст. 6(1)(f) GDPR как на законное основание для обработки данных? В этом контексте, может ли контролер данных опираться на ст. 6(1)(f) GDPR при раскрытии персональных данных? Если правоохранительные органы за пределами ЕС не могут опираться на ст. 6(1)(f) GDPR как на законное основание для обработки данных, на какое законное основание могут опираться правоохранительные органы за пределами ЕС?

В целом Bird & Bird сообщила следующее:

1. Для применения статьи 6(1)(c) должен существовать «закон объединения или право государства-члена, которому подчиняется контролер», и поэтому данное основание имеет ограниченное применение, если LEA находится за пределами юрисдикции контролера.
2. Из шести законных оснований для обработки персональных данных, перечисленных в статье, 6(1)(a) «Согласие», 6(1)(b) «Контракт», 6(1)(d) «Жизненные интересы человека» и 6(1)(e) «Общественные интересы или официальные органы» вряд ли применимы к запросам LEA.
3. Статья 6(1)(f) «Законный интерес» может быть применимым основанием для контролера, когда правоохранительный орган, не входящий в ЕС, делает запрос на получение персональных данных от контролера в ЕС.
4. Если LEA находятся за пределами ЕЭЗ, их законное основание для обработки в соответствии с GDPR не имеет значения, поскольку они не подпадают под действие

GDPR. Организации, раскрывающие данные правоохранительным органам за пределами ЕЭЗ, по-прежнему будут нуждаться в имеющем законную силу основании, которое позволяло бы это делать. В случае ICANN таким основанием, как правило, является законный интерес.

5. Если деятельность СР регулируется GDPR, но эта сторона находится за пределами ЕЭЗ, она также будет подчиняться местному законодательству. Это означает, что контролеры могут столкнуться с правовой коллизией.

1. Может ли контролер данных опираться на статью 6(1)(c) GDPR для раскрытия персональных данных правоохранительным органам за пределами юрисдикции контролера данных?

- Обработка, необходимая для соблюдения юридического обязательства, которому подчиняется контролер, доступна только в том случае, если юридическое обязательство изложено в законодательстве ЕС или государства-члена.
- Если на контролера распространяются обязательства по раскрытию информации, вытекающие из законов юрисдикций за пределами ЕС, контролер не может опираться на статью 6(1)(c).
- В соответствии с законодательством ЕС или государства-члена контролер может быть связан юридическим обязательством раскрывать персональные данные правоохранительным органам, не входящим в ЕС.
- MLAT могут охватывать это, но когда приходит запрос там, где действует MLAT, контролер должен отклонить этот запрос и обратиться к MLAT. Если нет MLAT или другого соглашения, контролер должен гарантировать, что раскрытие информации третьей стране не будет нарушением местного законодательства.

2. Может ли контролер данных опираться на любые другие правовые основания, помимо ст. 6(1)(f) GDPR, для раскрытия персональных данных правоохранительным органам за пределами юрисдикции контролера данных?

- Пункты 6(1)(f) и 6(1)(c) могут применяться, но остальные пять законных оснований для обработки персональных данных, скорее всего, нет.
- Если правоохранительный орган, не входящий в состав ЕС, обращается с запросом на получение персональных данных от контролера в ЕС, он может продемонстрировать законный интерес (6(1)(f)) в раскрытии данных. EDPB также предложила этот подход в переписке с ICANN (например, EDPB-85-2018).

3. Могут ли правоохранительные органы за пределами ЕС опираться на статью 6(1)(f) GDPR как на законное основание для обработки данных? В этом контексте, может ли контролер данных опираться на статью 6(1)(f) GDPR при раскрытии персональных данных? Если правоохранительные органы за пределами ЕС не могут опираться на статью 6(1)(f) GDPR как на законное основание для обработки данных, на какое законное основание могут опираться правоохранительные органы за пределами ЕС?

- Как субъекты страны, правоохранительные органы защищены государственным иммунитетом, и поэтому правоохранительные органы, находящиеся за пределами ЕС, не подпадают под действие GDPR.
- Даже если предположить, что GDPR может применяться к правоохранительным органам за пределами ЕС, кажется маловероятным, что правоохранительные органы за пределами ЕС рассматривали бы возможность обоснования своей обработки данных в соответствии с GDPR.
- Следовательно, правоохранительным органам, не находящимся в ЕС, не нужно оценивать, на какое законное основание GDPR они опираются при обработке данных.
- Контролер, который передает данные LEA за пределы ЕС, тем не менее, должен будет подумать о том, как выполнить обязательства, изложенные в главе V (передача персональных данных третьим странам или международным организациям).

Вопрос 5 (Псевдонимизированные адреса электронной почты)

Группа обсудила вариант замены адреса электронной почты, предоставленного субъектом данных, альтернативным адресом электронной почты, который сам по себе не идентифицирует субъекта данных (пример: sfjgsdfsafgkas@pseudo.nym). При таком подходе в ходе обсуждения возникли два варианта, где (a) одна и та же уникальная строка будет использоваться для нескольких регистраций субъекта данных («псевдонимизация») или (b) строка будет уникальной для каждой регистрации («анонимизация»). В соответствии с вариантом (a) личность субъекта данных может — но не обязательно — быть идентифицирована посредством перекрестных ссылок на содержимое всех регистраций доменных имен, для которых используется строка.

Исходя из этих вариантов, возник следующий вопрос: В вариантах (a) и (или) (b) следует ли рассматривать альтернативный адрес как персональные данные субъекта данных в соответствии с GDPR, и каковы будут правовые последствия и риски этого определения в отношении предлагаемой публикации этой строки в общедоступном разделе службы регистрационных данных (RDS)?

Краткий ответ Bird & Bird

Мы считаем, что любой вариант ((a) или (b)) по-прежнему будет рассматриваться как публикация персональных данных в интернете. Похоже, что такой случай охвачен в заявлении, сделанном в заключении Рабочей группы 29-й статьи от 2014 года о методах анонимизации [ec.europa.eu]: «когда контролер данных не удаляет исходные (идентифицируемые) данные на уровне события, а передает часть этого набора данных (например, после удаления или маскирования идентифицируемых данных), результирующий набор данных по-прежнему является персональными данными». Цель сделать этот адрес электронной почты доступным, даже если он замаскирован, по-видимому, состоит в том, чтобы позволить третьим сторонам напрямую связываться с субъектом данных (например, чтобы вручить судебную повестку, потребовать прекращения работы домена и так далее), поэтому он довольно четко связан с этим конкретным субъектом данных, по крайней мере, в том, что касается ICANN и сторон, связанных договорными обязательствами. Тем не менее, любой вариант рассматривался бы как ценная технология повышения конфиденциальности (OPET)/принцип «privacy by design».

Вопрос 6 (Согласие)

Регистрационные данные, представленные владельцами доменов-юридическими лицами, могут содержать данные физических лиц. В меморандуме фазы 1 говорилось, что регистраторы могут полагаться на самоидентификацию владельца домена как юридического или физического лица, если риск снижен путем принятия дальнейших мер для обеспечения точности обозначения владельца домена. В продолжение этого меморандума: какие варианты согласия и требования связаны с такими обозначениями? В частности: вправе ли контролеры данных полагаться на заявление, обязывающее владельцев доменов-юридических лиц получить согласие у физического лица, которое будет действовать в качестве контактного лица и чья информация может быть публично отображена в RDS? Если да, то какие заверения, если таковые имеются, было бы полезно получить контролеру от владельца домена-юридического лица в этом случае?

В рамках вашего анализа мы предлагаем ознакомиться с политикой GDPR и практикой регистратуры IP-адресов RIPE-NCC (европейская регистратура, расположенная в Нидерландах). Клиенты RIPE-NCC (владельцы доменов) — это юридические лица, публично отображаемые в WHOIS. RIPE-NCC возлагает на своих владельцев доменов-юридических лиц ответственность за получение разрешения у этих физических лиц и предлагает для этого процедуры и механизмы защиты. Заявленные RIPE-NCC обоснование миссии и целей сбора данных аналогичны указанным во Временной спецификации ICANN. Могут ли подобные политики и процедуры использоваться в ICANN?

Также мы предлагаем ознакомиться с политикой ARIN, регистратуры IP-адресов для Северной Америки. Некоторые клиенты ARIN находятся в ЕС. ARIN тоже публикует данные физических лиц в своей базе данных WHOIS. Клиентами ARIN являются физические лица, которые предоставляют контактные данные физических лиц.

Краткий ответ Bird & Bird

В этом документе анализируются требования к согласию, изложенные в GDPR, и изучаются варианты согласия для целей публикации в RDS персональных данных, предоставленных в контексте регистрации владельцев доменов-юридических лиц.

Требования к согласию

В соответствии с GDPR согласие должно быть добровольным, конкретным, информированным и недвусмысленным. Кроме того, оно должно быть получено до начала обработки. Контролеры должны иметь возможность продемонстрировать, что действительное согласие было дано, и что физические лица имеют право отозвать согласие в любое время. Согласно GDPR, обязанность получить согласие лежит на контролере. Контролер может дать указание третьей стороне получить согласие

физических лиц от его имени; однако это не освобождает контролера от его обязательств в соответствии с GDPR.

Варианты согласия

На основе вышеуказанных требований в этом документе рассматриваются следующие варианты получения согласия на публикацию персональных данных в RDS и излагаются соображения по соответствию каждого варианта обязательствам:

1. Контролеры запрашивают действительное согласие напрямую у физических лиц
    - Публикация персональных данных в RDS не является обязательной.
    - Перед публикацией персональных данных контролер напрямую связывается с физическими лицами, чтобы получить согласие в соответствии с GDPR.
    - В случае отказа дать согласие или отсутствия ответа персональные данные не будут опубликованы.

2. Владелец домена получает действительное согласие и предоставляет доказательства контролеру.
    - Публикация персональных данных в RDS не является обязательной.
    - Перед публикацией персональных данных контролер требует от владельца домена: (a) получить согласие физических лиц; а также (b) предоставить контролеру доказательства того, что согласие было получено.
    - В случае отказа дать согласие или при отсутствии доказательств персональные данные не будут опубликованы.

3. Владелец домена получает действительное согласие, а контролер удостоверяется в этом, обратившись к физическому лицу.
    - Перед публикацией персональных данных контролер требует от владельца домена: (a) получить согласие физических лиц; а также (b) предоставить контролеру доказательства того, что согласие было получено.
    - Контролер напрямую связывается с физическим лицом: он информирует его о получении от владельца домена подтверждения согласия этого лица.

4. Владелец домена обязуется получить согласие
    - Владельцам доменов разрешается предоставлять контактные данные, не являющиеся персональными.
    - Регистрационные данные публикуются по умолчанию (независимо от того, включены ли в их состав персональные данные).
    - Посредством заявления владельцы доменов обязуются получать согласие физических лиц в случае предоставления персональных данных.

Вопрос 7 (Точность)

Вопрос 1a

Кто имеет право ссылаться на принцип точности? Мы понимаем, что целью принципа точности является защита субъекта данных от вреда в результате обработки недостоверной информации. Имеют ли право ссылаться на принцип точности в соответствии с GDPR другие лица, такие как стороны, связанные договорными обязательствами, и ICANN (в качестве контролеров), правоохранительные органы, правообладатели ИС и так далее? Отвечая на этот вопрос, не могли бы вы прояснить стороны/интересы, которые мы должны учитывать в целом и, в частности, при интерпретации следующих положений предыдущих меморандумов:

- В обоих меморандумах в нескольких разделах упоминаются «соответствующие стороны». Ограничен ли круг «соответствующих сторон» контролерами или мы должны также учитывать интересы третьих сторон?
    - «Могут возникнуть вопросы относительно того, достаточно ли RNH или владельцу учетной записи подтвердить точность информации, касающейся технических и административных контактов, не запрашивая информацию у таких контактных лиц напрямую. GDPR не обязательно требует, чтобы в случаях, когда персональные данные должны быть проверены, они проверялись самим субъектом данных. ICANN и соответствующие стороны могут полагаться на третьи стороны для подтверждения точности персональных данных, если это разумно. Поэтому мы не видим непосредственных причин считать текущие процедуры недостаточными». (выделение добавлено) (пункт 19 — Точность)
    - «В общей сложности, так как в основе соблюдения принципа точности данных лежит разумная необходимость, оценку достаточности этих процедур уместнее выполнить ICANN и соответствующим сторонам. С нашей точки зрения, поскольку эти процедуры требуют активных действий, которые будут способствовать подтверждению точности, если нет оснований считать эти меры недостаточными, мы не видим очевидной необходимости в их пересмотре». (выделение добавлено) (пункт 21 — Точность)
    - «Если бы у соответствующих сторон не было причин сомневаться в надежности самоидентификации владельца домена, то они, вероятно, могли бы полагаться только на самоидентификацию без независимого подтверждения. Однако мы понимаем, что стороны обеспокоены тем, что некоторые владельцы доменов не поймут вопрос и будут ошибочно идентифицировать себя. Поэтому возникнет риск ответственности, если соответствующие стороны не предпримут дальнейших шагов для обеспечения точности обозначения владельца домена». (выделение добавлено) (пункт 17 — Юридические и физические лица)

1.b Аналогичным образом, в меморандуме по вопросу разграничения юридических и физических лиц указано на «важность» данных при определении уровня усилий, необходимых для обеспечения точности. Ограничивается ли оценка «важности» данных рассмотрением важности для субъекта данных и контролера (контролеров), или она также включает важность данных для третьих лиц (в данном случае это правоохранительные органы, правообладатели ИС и другие лица, которые будут запрашивать данные у контролера для своих целей)?

- «Как поясняется в руководстве ICO: «Чем важнее точность персональных данных, тем больше усилий вы должны приложить для обеспечения их точности. Поэтому, если вы используете данные для принятия решений, которые могут существенно повлиять на конкретного человека или на других лиц, вам нужно приложить больше усилий для обеспечения точности» (пункт 14 — Юридические и физические лица).

Основные положения Bird & Bird

В этом документе рассматриваются дальнейшие соображения в отношении принципа точности (стороны, обязанные соблюдать этот принцип, лица, которые имеют право ссылаться на него, и необходимая основа для оценки точности данных). В нем изложены факторы, которые следует учитывать при оценке точности данных, и даны рекомендации по мерам повышения точности регистрационных данных, хранящихся у сторон, связанных договорными обязательствами.

Стороны, подпадающие под действие принципа точности, и «соответствующие стороны»

Согласно GDPR, обязанность получить согласие лежит на контролере. Ссылки на «соответствующих сторон» в меморандумах «Точность» и «Юридические и физические лица» относятся к соответствующим контролерам данных WHOIS.

Стороны, имеющие право ссылаться на принцип точности

GDPR предусматривает ряд средств правовой защиты: жалобы в надзорные органы, средства судебной защиты и право на компенсацию со стороны контролера или стороны, ответственной за обработку данных. Субъекты данных (и, если это разрешено национальным законодательством, их представители) имеют право использовать все средства правовой защиты, указанные в GDPR. В некоторых случаях эти права также могут быть реализованы другими физическими или юридическими лицами, например, теми, кого затрагивает решение надзорного органа, или теми, кому был причинен ущерб в результате нарушения GDPR.

Интересы различных сторон при рассмотрении точности

Цель обработки персональных данных имеет значение при определении мер, необходимых для обеспечения точности данных. При оценке точности данных необходимо учитывать интересы субъекта данных. В некоторых случаях интересы контролера также будут иметь значение. Хотя в руководстве ICO по вопросу точности есть несколько ссылок на права «других», этот момент не получил дальнейшего освещения в рассмотренных нами рекомендациях, прецедентном праве или литературе. Учитывая отсутствие указаний, мы не рекомендуем уделять этому моменту слишком много внимания.

Разумные меры по обеспечению точности данных

Принцип точности не был подробно исследован в литературе и прецедентном праве, и ссылки на него ограничены. Разумный и надлежащий характер показателей точности следует рассматривать в свете подхода GDPR, основанного на оценке риска, с учетом, среди прочего, цели и последствий обработки. Список предлагаемых мер точности изложен в этом документе.

Вопрос 8 (Примеры использования автоматизации)

Справочная информация

1. В первом сценарии автоматизация будет осуществляться в центральном шлюзе, которому поручено получать запросы от аккредитованных пользователей. Центральный шлюз будет давать автоматические рекомендации о том, следует ли раскрывать запрашиваемые данные, в то время как окончательное решение о раскрытии данных будет приниматься сторонами, связанными договорными обязательствами, которые могут либо следовать рекомендации, либо нет (Сценарий 1.a.). Стороны, связанные договорными обязательствами, достаточно доверяющие шлюзу, могут автоматизировать принятие решений о раскрытии данных (Сценарий 1.b.).

2. Согласно второму сценарию решение о раскрытии данных владельца домена будет приниматься центральным шлюзом без возможности рассмотрения запроса стороной, связанной договорными обязательствами. Центральный шлюз примет это решение либо (i) после получения соответствующих данных от стороны, связанной договорными обязательствами, и оценки данных в рамках принятия решения (Сценарий 2.a.), либо (ii) без получения данных владельца домена (в этом случае решение будет основано исключительно на информации о подателе запроса и утверждениях, сделанных в запросе) (Сценарий 2.b.). Одним из примеров последнего сценария может быть автоматизированное раскрытие регистрационных данных microsoft-login.com проверенному владельцу товарного знака MICROSOFT в ответ на запрос, в котором утверждается о нарушении прав на товарный знак и выражается намерение обработать данные для обоснования, подачи или защиты от юридических претензий. Нас попросили предположить, что в каждом сценарии будет задействован ряд механизмов защиты, которые включены в этот меморандум в качестве Приложения 1.

A. Примеры использования в сценарии 1:

В свете рекомендаций, ранее предоставленных в меморандумах по вопросам 1 и 2 (Ответственность) и вопросу 3 (Автоматизация), мы просим представить следующий анализ каждого примера использования в Приложении 1:

1. Опишите риск ответственности для центрального шлюза и сторон, связанных договорными обязательствами («СР»), сопряженный с автоматизацией этой рекомендации, а также с автоматизацией принятия решения о раскрытии персональных данных третьей стороне. Если для оценки риска требуется дополнительная информация, укажите необходимую дополнительную информацию.

2. Является ли решение о раскрытии персональных данных третьей стороне решением, «которое имеет юридические последствия в отношении [субъекта данных] или аналогичным образом существенно влияет на него или ее» в рамках статьи 22?

3. Существуют ли дополнительные меры или механизмы защиты, которые снизили бы риск ответственности?

4. Влияет ли автоматизированное принятие решений, реализованное таким образом, на ваш анализ ролей/ответственности сторон, описанных в меморандуме по вопросам 1 и 2 (например, стороны, связанные договорными обязательствами, остаются ответственными контролерами, если «раскрытие информации происходит автоматически, без какого-либо ручного вмешательства». 1.1.4).

B. Примеры использования в сценарии 2:

Во втором (альтернативном) сценарии, когда центральный шлюз имеет закрепленную договором возможность потребовать от сторон, связанных договорными обязательствами, предоставить данные центральному шлюзу:

1. Как альтернативные сценарии влияют на анализ, представленный в вопросах с 1 по 4 выше?

2. Какой сценарий предполагает наименьший риск ответственности для сторон, связанных договорными обязательствами? Мы просим в ответе изложить ваши предположения относительно соответствующих ролей ICANN и сторон, связанных договорными обязательствами, включая сценарий, при котором центральный шлюз передал принятие решений на аутсорсинг независимому поставщику юридических услуг.

C. Дополнительные пояснения по автоматизации

1. Если решение о раскрытии персональных данных третьей стороне автоматизировано, каким образом контролеры должны предоставлять владельцу домена информацию о возможности автоматического принятия решения при обработке его или ее персональной информации? Как эта информация должна доводиться до сведения владельца домена и какую информацию, относящуюся к автоматизированному принятию решений, необходимо передать владельцу домена, чтобы обеспечить справедливую и транспарентную обработку в соответствии со статьей 13?

2. Влияет ли предоставление контролерами информации в ответе на вопрос C.1 выше на право владельца домена получить подтверждение о том, имело ли место автоматизированное принятие решения о раскрытии его персональных данных третьей стороне? Влияет ли это на право владельца домена на получение соответствующей значимой информации в соответствии со статьей 15.1(h)?

3. Влияет ли способ принятия решения, описанный выше, на способ предоставления этой информации?

4. Какую роль ближайшая причина играет в определении того, имеет ли решение о раскрытии юридические или аналогичные значимые последствия (то есть насколько решение о раскрытии персональных данных владельца домена должно быть связано с окончательным юридическим или аналогичным значимым эффектом обработки персональных данных)? Пожалуйста, опишите риск ответственности перед центральным шлюзом или стороной, связанной договорными обязательствами, если после получения персональных данных податель запроса начнет свою собственную обработку, которая имеет юридические или аналогичные значимые последствия.

5. В разделе 1.12 предыдущего меморандума по автоматизации Bird & Bird утверждала: Также можно структурировать SSAD таким образом, чтобы она не требовала «принятия решения исключительно на основании автоматизированной обработки». Подробнее: SSAD, вместо того, чтобы запрашивать информацию у подателей запросов и оценивать, выполняются ли соответствующие критерии разглашения закрытых регистрационных данных, SSAD может публиковать категории допустимых запросов и запрашивать у подателей запросов подтверждение того, что они соответствуют установленным критериям. В этом случае не было бы автоматизированной обработки, приводящей к решению раскрыть данные. SSAD могла бы предлагать подателям запросов предоставить дополнительную информацию о характере их запроса для целей аудита, которая не будет использоваться для оценки самого запроса. Не могли бы вы подробнее рассказать о том, как (i) публикация категорий запросов, которые будут утверждены, и (ii) требование, чтобы податель запроса вручную выбирал применимую категорию и подтверждал, что он соответствует критериям для этой категории запросов, сделает решение о раскрытии «не автоматизированным»?

Основные положения Bird & Bird

В этом документе рассматриваются сценарии и примеры использования, представленные Группой по EPDP в отношении автоматизированных решений о разглашении закрытых данных владельцев доменов. Определены случаи полностью автоматизированных решений, которые подпадают под действие ст. 22 GDPR, проблемы, связанные со ст. 22, и доступные альтернативы. В документе также предлагаются механизмы защиты данных и рассматриваются соображения транспарентности в контексте SSAD. И наконец, в нем исследуется статус сторон для каждого сценария и связанный с этим риск ответственности.

Ст. 22: решения и альтернативы

Ст. 22 GDPR применяется к полностью автоматизированным решениям, которые имеют юридические или аналогичные значимые последствия. Решения в рамках ст. 22 разрешено принимать только в ограниченных случаях, которые вряд ли применимы в контексте SSAD. Полная автоматизация решений разрешена только в том случае, если они: (a) не предусматривают обработку персональных данных; (b) не вызывают

юридических или аналогичных значительных последствий; (c) разрешены применимым законодательством ЕС или государства-члена, которое устанавливает подходящие меры для защиты людей; или (d) подпадают под действие национального исключения из ст. 22 (например, с целью раскрытия уголовных преступлений). Во всех остальных случаях необходимо значимое участие человека в процессе принятия решений.

Применимы ли критерии ст. 22 к SSAD?

(a) Полностью автоматизированная обработка: Для применения ст. 22 требуется некоторая обработка персональных данных, но нет требования, чтобы для принятия решения обрабатывались только персональные данные. Рассматриваемое здесь решение в большинстве случаев будет включать обработку персональных данных — это будет иметь место независимо от того, есть ли у центрального шлюза доступ к запрошенным данным и учитывает ли он такие данные при принятии решения. За исключением сценария 1.a, где SSAD будет выдавать только автоматические рекомендации, все остальные сценарии будут включать решение (раскрыть данные владельца домена третьим сторонам), основанное исключительно на автоматизированной обработке.

(b) Юридические или аналогичные значимые последствия: термин не определен в GDPR; однако это указывает на повышенный порог. Будет ли раскрытие данных владельца домена иметь такие последствия, зависит от обстоятельств запроса: в документе оценивается характер последствий раскрытия для каждого примера использования. Мы дали четкие ответы «да» и «нет» там, где это возможно: некоторые примеры использования выиграют от дальнейшего обсуждения. Роль ближайшей причины в определении последствий решения не рассматривалась судами или надзорными органами. В немецкой литературе ведутся некоторые дискуссии; однако, учитывая отсутствие более широкого обсуждения, мнения надзорных органов на эту тему могут быть полезны, поскольку это может позволить автоматизировать SSAD на том основании, что центральный шлюз/CP принимают только предварительное решение.

Механизмы защиты

Список предлагаемых механизмов защиты данных приведен в Приложении 2 к настоящему документу. Сюда входит, среди прочего: взаимодействие с надзорными органами, четкое определение рамок каждого примера использования и создание правовой основы, установление соответствующих условий раскрытия информации для подателя запроса, внедрение соответствующих мер безопасности, принятие мер по соблюдению принципа подотчетности, установление политики для удовлетворения требований физических лиц и заключение соответствующих положений о защите данных со сторонами, ответственными за обработку данных.

Транспарентность

Способ предоставления информации не зависит от наличия автоматизированного принятия решений, но содержание информации зависит.

- Информация обычно предоставляется через уведомление о конфиденциальности; учитывая важность SSAD в системе доменных имен, было бы целесообразно использовать способ, обеспечивающий привлечение внимания.
- Эффективнее всего справиться с задачей предоставления соответствующей информации могли бы регистраторы (учитывая их прямые отношения с владельцами доменов), независимо от того, считаются ли они контролерами в контексте SSAD. Если они не являются контролерами, но предоставляют информацию от имени контролера, это следует прояснить для владельцев доменов.
- Что касается содержания (только для решений по ст. 22), уведомление также должно содержать информацию о существовании автоматизированного решения и задействованной логике, а также о значимости и предполагаемых последствиях обработки.
- Элементы ст. 15 GDPR (право доступа) необходимо предоставлять по запросу, даже если они уже были включены в уведомление.
- Право доступа требует, чтобы контролеры предоставляли сведения о получателях, которым данные «были или будут раскрыты»: это означает, что при отсутствии применимых исключений необходимо информировать владельцев доменов, воспользовавшихся своим правом доступа, о раскрытии их данных третьим сторонам.

Статус сторон

(a) Согласно сценарию 1 окончательное решение о раскрытии данных владельца домена остается за CP. Анализ, проведенный в меморандуме об ответственности, здесь также будет иметь место, и, скорее всего, CP будут рассматриваться надзорными органами как контролеры, совместно отвечающие за обработку данных с ICANN.

(b) По сценарию 2 ситуация менее ясна. В зависимости от того, принят ли макро- или микроуровневый подход, CP могут быть контролерами, (совместно) отвечающими за обработку данных для автоматизированного принятия решений и раскрытия данных подателям запросов или просто для раскрытия данных центральному шлюзу. Мы думаем, что второй вариант (контролеры только для раскрытия данных центральному шлюзу) является более правильным выводом, но суть не ясна. Передача решения на аутсорсинг независимому поставщику юридических услуг вряд ли изменит вышеуказанное положение.

В обоих сценариях утверждение, что CP являются сторонами, ответственными за обработку данных, было бы неубедительным.

Ответственность CP рассматривается в отношении:

(a) статуса CP: если CP являются контролерами, совместно отвечающими за обработку данных, важно четко распределить задачи и обязанности посредством соглашения;
(b) типа ответственности:

- Ответственность перед физическими лицами: правилом является солидарная ответственность, и CP могут нести ответственность за весь ущерб, причиненный обработкой, в которой они участвуют, независимо от их статуса. Они могут избежать этого, только продемонстрировав, что они никоим образом не причастны к событию, которое привело к ущербу. В противном случае они имеют право потребовать от других контролеров возврата части компенсации, соответствующей их ответственности.
- Ответственность перед надзорными органами: солидарная ответственность здесь менее очевидна, и есть основания утверждать, что принудительные меры должны применяться на основе «степени ответственности» стороны.

С точки зрения риска сценарий 2, по-видимому, представляет меньший риск ответственности как в отношении компенсации физическим лицам, так и в отношении принудительных мер со стороны надзорных органов.